BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Unità di Informazione Finanziaria Annual Report

Rome, May 2018

year 2017

number 10

BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Unità di Informazione Finanziaria Annual Report

2017

Roma, May 2018

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

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

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

Unità di Informazione Finanziaria per l'Italia

Director
Claudio Clemente

Address
Largo Bastia, 35
00181 Rome – Italy

Telephone
+39 0647921

Website
http://uif.bancaditalia.it

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

Printed in June 2018 by the Printing and Publishing Division of the Bank of Italy.

CONTENTS

List of boxes:

INTRODUCTION

On 4 July 2017, the modifications to the national anti-money legislation were completed with the entry into force of the rules for transposing the fourth EU AML Directive.

Thanks to its first ten years of experience and the consolidation of its role, the UIF made a significant contribution to the various phases of drawing up the legislation, making proposals also at parliamentary level for additions and modifications to increase the effectiveness of the system, specifically by broadening the scope for information exchanges and the cooperation between all parties concerned, both public and private. The acceptance into the Committees' opinions of many of the indications provided by the UIF was not fully reflected in the legislative decree subsequently issued, which left various areas of uncertainty that now need to be resolved through the practical application of the rules.

The legislative reform also introduced significant changes to the UIF's tasks, and the Unit immediately began working to adapt to them.

The new procedures for cooperating with the National Anti-Mafia and Anti-Terrorism Directorate were the subject of specific memorandums of understanding. Guidelines were provided for the anti-money laundering contribution requested from general government entities in their renewed role which sees the UIF as the main interlocutor. The interventions necessary to introduce threshold-based communications were prepared; they will expand the Unit's information set as is happening in several foreign systems, following a phase of dialogue with representatives of the parties concerned. Discussions began with the regulatory and self-regulatory bodies to draw up the regulations and decide how to implement them across the various sectors. At international level, significant efforts continued at regulatory and operational level towards harmonization and overcoming the differences that are currently hindering effective cooperation between the FIUs (Chapter 1).

Looking ahead, the application of the new rules and the extension of the list of obliged entities should further increase the number of suspicious transaction reports, which numbered around 94,000 at the end of last year, after the peak recorded in 2016 (101,000 reports) due to the extraordinary component linked to the voluntary disclosure procedures. Net of this component, the growth in reports continued in 2017 too with an increase of 9.7 per cent, the highest in the last three years. In the current year, the number of reports analysed by the Unit and sent to the investigative authorities exceeded the number received, which made it possible to further reduce the backlog, although serious inroads had already been made (see Chapters 2 and 3).

As far as quality is concerned, the intelligence cycle will be able to take advantage of the regulatory changes that envisage access for the UIF to investigative data and an expansion in feedback on reports, thereby providing reporting entities with more information. In 2017, the Unit continued its work on identifying anomalous operational schemes that are not easily recognized by obliged entities, and on analysing complex cases, which allowed new investigations to be launched and

provided important support for ongoing investigations. The results achieved are encouraging the UIF to continue in this direction in order to contribute further to the growth of the system (Chapter 4).

There was a considerable increase (+58 per cent) in reports on the financing of terrorism, which numbered almost 1,000. A contributory factor to this growth was the awareness-raising initiative for reporting entities carried out by the UIF based on the most recent episodes (Chapter 5).

Analyses and studies continued and also made use of new databases: encouraging results in terms of identifying anomalous flows to other countries emerged from a comparison of the official statistics on foreign trade. The work carried out contributes to assessing the money laundering risks faced by operators, helps to update the National Risk Assessment, and guides control and inspection activities (Chapter 6).

The constant expansion of the list of obliged entities is prompting a targeted use of inspections to verify compliance with active cooperation obligations on the part of those categories particularly exposed to money laundering risks or that are less expert in identifying anomalies. There were significant changes to the sanction system in terms of those liable, the competent authorities, the classification of violations and the amount of the sanctions, all of which require changes to the investigations and the sanction imposition procedures (Chapter 7).

Cooperation with the other authorities was further strengthened, due to both the new provisions that increased the Unit's direct interlocutors and the operational requirements that led to a sharp increase in relations with the supervisory organizations, the Finance Police, the Anti-Mafia Investigation Department and various public prosecutors (Chapter 8).

A more fruitful international cooperation is promoted by the strengthening of the role of the EU FIUs Platform, a goal actively pursued by the Unit in order to facilitate information exchanges and carry out joint analyses on cases of common interest (Chapter 9).

The greater commitments arising from the changed regulatory framework, from the expected further developments and from the central role assigned to the FIUs by the international rules mean changes to the Unit's strategic and organizational guidelines. They represent a new challenge for its staff, already committed to working with the passion and preparedness that have distinguished the first ten years of the UIF's work and enabled it to make an increasingly effective contribution to the fight against financial crime (Chapter 10).

The Director

Claudio Clemente

1. THE LEGISLATIVE FRAMEWORK

1.1. The evolution of the international framework

The past year was marked in Europe by the creation of initiatives designed to accompany the effective implementation of the Fourth Directive and to extend and complete the regulatory framework to take account of both the problems emerging from operational experience and the changes in risks, which require new and more adequate measures in line with the changes in international standards and policy.

The Fourth EU AML Directive[1] introduced significant innovations into European law, requiring a significant effort on the part of the Member States to implement it. Most countries have either completed or are close to completing the transposition into national law, in part thanks to the impulse given by the European Commission.

The Fifth EU AML Directive

On 13 December 2017, the European Commission, Council and Parliament reached an agreement on the text of the Fifth EU AML Directive. Its adoption is one of the main objectives of the European Commission's Action Plan to combat the financing of terrorism.

The Fifth Directive broadens the range of subjects under anti-money laundering obligations including, among others, providers of exchange services between virtual and 'fiat' currencies and wallet providers for keeping credentials for access to virtual currencies. There are forms of registration and control envisaged for both categories of operator.

As regards customer due diligence: identification is possible using electronic instruments and processes recognized and regulated at national level; the cases where enhanced due diligence measures must be applied are specified and extended, especially for counterparties from third countries identified as being at 'high risk' on the European 'black list'; the safeguards for prepaid cards are extended by lowering the exemption thresholds and establishing that cards issued in third countries can only be used in the EU if their characteristics are equivalent to those set out by the Directive; and an explicit ban on the anonymous ownership of safe-deposit boxes has been introduced.

For greater transparency on beneficial ownership, the Fifth Directive broadens the range of information in the relative registers and extends accessibility to the information they contain. It clearly sets out the need to register, as well as companies and trusts (including 'family' trusts), any entities similar to the latter. It also provides that trusts must be entered in the register of the State where the trustee is resident.

The FIUs have full and unconditioned access to the registers, on a par with the other competent authorities. Access for the general public, though limited to a part of the information, is extended and the requirement of the 'legitimate interest' is removed (except for information about trusts). Where it does not interfere with their functions, obliged entities and competent authorities are required to report any

[1] Directive (EU) 2015/849.

discrepancies found between the content of the registers and the information they have. For the FIUs, this disclosure is limited by the confidentiality of information concerning STRs and analyses.

Specific provisions in the new Directive concern the information-gathering powers of the FIUs for domestic analysis and for international cooperation.

The FIUs must be able to get information from any obliged entity, regardless of the existence of a prior suspicious transaction report. It must be possible to acquire this information directly and by making a simple request, with no limits imposed by national rules and procedures (for example due to conditions or authorizations). The Directive aims at enhancing the capacity of FIUs to cooperate at international level, excluding constraints and grounds for refusal that frequently occur in practice (such as connections with tax matters or the existence of confidentiality regimes, investigations or criminal proceedings).

The Fifth Directive entrusts the Commission with monitoring developments in the operational activity and the cooperation among European FIUs and with proposing corrective measures. The Commission is called on to assess this cooperation system, paying particular attention to existing obstacles and to the improvements that need to be introduced, also by establishing a 'coordination and support mechanism'.[2]

The 'PANA Committee' Report

In terms of preventing and combating financial crimes, in December 2017 the European Parliament approved the Final Report of the 'PANA Committee', set up in 2016 to deal with the problems brought to light by the 'Panama Papers' case. The Report is accompanied by twenty-one Recommendations for the European Council and Commission. The UIF contributed to the Committee's work by taking part in a hearing on the characteristics, activities and cooperation of European FIUs.

The Committee's Recommendations call for improved effectiveness in action and cooperation between FIUs, a greater convergence in their functions and powers and the creation of a more effective information exchange system, also through the establishment of a European FIU. Among other things, the Report is based on the results of the 'Mapping Exercise and Gap Analysis on FIUs' Powers and Obstacles for Obtaining and Exchanging Information', promoted and coordinated by the UIF on the EU FIUs Platform[3] and indicated by the ECOFIN Council as the instrument on which to base new policies and rules to strengthen the FIUs and a benchmark for further measures and interventions. A centralized European body could encourage closer cooperation through more extensive information sharing and more joint analyses, although the tasks of receiving, analysing and disseminating STRs that FIUs carry out in order to identify illegal activities, are of necessity carried out at national level.

---

[2] Article 65(3) of the Fourth Directive, as modified by the Fifth Directive: 'The Commission shall assess the framework for FIUs' cooperation with third countries and obstacles and opportunities to enhance cooperation between FIUs in the Union including the possibility of establishing a coordination and support mechanism'.

[3] The Mapping Exercise analysed the various national frameworks characterizing the organization, the powers and activities of the FIUs and showed the effects of the low level of harmonization on the quality of the analyses and mutual cooperation. See Annual Report of the UIF on activities carried out in 2016, Chapter 9.

1.1.1. Other areas for development and ongoing tasks

There is growing interest in the international community in developing forms of cooperation to strengthen the coordination and sharing of information between public authorities at domestic level, and in creating better ways for public institutions and the private sector to communicate and cooperate.

The Report on Effective Inter-Agency Co-Operation in Fighting Tax Crimes

The Report on 'Effective Inter-Agency Co-Operation in Fighting Tax Crimes and Other Financial Crimes' by the OECD Task Force on Tax Crimes, now in its third edition, identifies the authorities which are contributing to the fight against financial crime in more than fifty countries, and reviews the characteristics and forms of national cooperation. The Report, to which the UIF contributed, makes recommendations to strengthen information exchanges and inter-institutional cooperation and also envisages tax agencies reporting any illegal acts found during their controls to the police or to the FIUs (specifically, tax evasion, corruption, money laundering and financing of terrorism). At the same time, to make the best use of these connections and enhance the effectiveness of combating on various fronts, the Report recommends access by tax administrations to information contained in STRs, in compliance with the applicable confidentiality rules.

The Ten Global Principles - OECD

As part of the Task Force, the UIF also helped to set down the 'Ten Global Principles' relating to improving the prevention and combating of tax crimes. Some of these principles take account of the anti-money laundering system too, underlining that tax crimes should always be included among the predicate offences of money laundering and that effective cooperation between the tax agencies and anti-money laundering authorities must be ensured at national and international level.

Cooperation between public authorities at national level

The FATF has also focused on inter-institutional cooperation, concentrating on the topic of 'Domestic inter-agency CFT information sharing', with a view to making information exchanges for preventing and combating the financing of terrorism more effective.[4] Similar measures are called for to strengthen cooperation in combating fiscal crimes.

Public-private cooperation

In 2017 the FATF was also committed to developing a broader dialogue between the public and private sectors to promote the exchange of information, the effectiveness of active cooperation and the quality of compliance.

A particularly thorough discussion took place at the Forum of FATF Heads of FIU[5] where, with the participation of private sector representatives, some national 'Financial Information Sharing Partnership' (FISP) models, based on structures and joint committees often coordinated by the FIUs, were presented and discussed.[6]

A comparative review shows the growing spread and development of public-private cooperation models in the anti-money laundering sector, albeit with considerable differences in the approaches adopted at national level, as regards both

[4] See the box 'Strengthening cooperation between authorities' in Section 5.3.
[5] See Section 9.6.
[6] Initiatives to promote more organized and systematic forms of public-private dialogue in the anti-money laundering sector are spreading rapidly to other international organizations as well, including the Egmont Group.

the authorities involved and the tasks carried out. The cooperation models set up in some English-speaking countries (Australia, Canada, Hong Kong, the United Kingdom, Singapore and the United States) are especially consolidated; they sometimes extend as far as sharing information on ongoing cases and handling them directly through joint analyses.

Italy's UIF, exploiting its administrative structure and its proximity to the financial system specifically and to obliged entities in general, has for some time engaged in various forms of dialogue with the private sector (e.g. about indicators and behaviour patterns for detecting suspicious transactions, reporting methods and report quality, feedback on specific cases or phenomena of a global nature, and problems with compliance).

The circulation of information among obliged entities

The FATF has also looked at how to extend the circulation of information in the private sector, with a view to promoting the assessment of money laundering and financing of terrorism risks, the application of appropriate customer due diligence measures and the effective and timely detection of suspicious transactions.

The circulation of information among obliged entities is conditioned by confidentiality constraints, which are more marked for the cross-border transmission of data, also because of the significant differences in national legislations. With the goal of promoting information sharing for assessing risks and identifying anomalies, in November 2017, the FATF published guidelines for the private sector (Private Sector Information Sharing), making it clear that the confidentiality constraints on STRs do not prevent infra-group information sharing.

Harmonization of the criminal offence of money laundering

Work continued throughout the year at European level on the adoption of a Directive aimed at harmonizing the criminal offence of money laundering, based on a European Commission proposal for implementing the 2016 Action Plan. This new criminal offence is in addition to, but does not replace, the administrative offence of money laundering contained in the Fourth Directive for prevention purposes.

The intervention aims to align EU legislation with the relevant international sources (the 2005 Warsaw Convention of the Council of Europe, and the FATF's Recommendations) through a common definition of money laundering behaviour and a minimum range of predicate crimes, with a view to fostering the convergence of national approaches and reducing the obstacles to cooperation between the competent authorities.

Negotiations for the new Regulation on declaring physical cash transfers

Negotiations have also continued on the draft of the new regulation on the declaration of physical transfers of cash,[7] specifically aimed at expanding the range of declaratory obligations[8] and broadening the information exchanges between the competent authorities, for cooperation at domestic and international level, especially between customs agencies and FIUs.

According to the draft regulation, declarations received by customs agencies must be sent promptly to the FIUs, rather than simply being 'made available' for possible acquisition or consultation, as provided for by the rules in force. The data

[7] Intended to replace EU Regulation 1889/2005.

[8] It foresees a broader definition of 'cash' to include, as well as banknotes and coins, bearer instruments, assets used as stores of value (such as gold) and prepaid payment cards.

gathered during border checks revealing links with criminal activity must follow the same regime as the declarations.

The 'black list' of third countries with strategic deficiencies

The European Commission's priorities include the commitment, provided for by the Fourth Directive, to identify those third countries that, owing to the strategic deficiencies in their national systems, are seen by the EU as having a high risk of money laundering or financing of terrorism.[9] Compiling and updating a 'black list' of third countries is a complex task that requires the broadest possible criteria (to avoid leaving room for gaps and subsequent arbitrage) that must also be strict to avoid excessive discretionality.

The European Parliament has openly criticized the approach underlying the Commissions' first 'delegated acts', through which the FATF's list of high-risk countries has simply been adopted. The Parliament has urged the Commission on more than one occasion to make a broader autonomous assessment of the jurisdictions with significant weaknesses as far as the EU is concerned. The Commission and the Member States, in light of the European Parliament's comments, are committed to drafting a dedicated methodology that can identify the shortcomings in all the main sectors of national anti-money laundering systems. The UIF is actively involved in this process.

Assessment of national legislation takes account of the elements highlighted in Article 9 of the Fourth Directive: the legal and institutional framework (especially regarding the crimes of money laundering and financing of terrorism); the powers of the competent authorities; and the adequacy of preventive measures. Attention has been focused on the need to extend the assessment to deficiencies in effectiveness (alongside the formal compliance of the legislation) and the measures to safeguard corporate and fiscal transparency and for international cooperation.

UNCAC Review

During the year, the UIF took part in the second cycle of the review of Italy's implementation of the United Nations Convention against Corruption (UNCAC). The exercise involved the chapters relating to prevention and asset recovery which contain, among other things, articles on the adequacy of the national anti-money laundering system.

The on-site visit by a team of experts in February 2017 was an opportunity to provide further information useful for a full understanding of how Italy's anti-money laundering system works. The Final Report is currently being prepared.

1.2. Risk assessment at European level

On 26 June 2017, the Commission published the first 'Report on supranational risk assessment'. This Supranational Risk Assessment is envisaged by the Fourth Directive as a constituent element of the overall risk-based approach characterizing the new rules.

[9] Article 9 of the Fourth Directive approved the dropping of the traditional approach based on a 'white list' of third countries having equivalent AML systems and tasked the Commission with compiling a 'black list' of countries at risk for Europe.

The FIUs contributed to the assessment both directly and through the European platform. The Unit shared the experience gained in the analysis of cross-border cases and of risks originating in other Member States.

The Report includes a comprehensive mapping of the risks by field of activity, a list of the methods most used by criminals for money laundering and the financing of terrorism, as well as the vulnerabilities common to all sectors (financial and non-financial). The assessment is completed by indicating the mitigation measures that the EU overall and each Member State should adopt to deal with the risks identified.

In the financial sector, private banking, custodial services (safe-deposit boxes), transfer of funds and currency exchange, electronic money, crowdfunding, virtual currencies and technological innovation (FinTech), consumer credit and the disbursement of small loans are indicated as sectors exposed to 'significant' or 'very significant' risks. As regards the non-financial sector, sources of risk are found in the following sectors: legal and accounting services, real estate, gambling (physical and online network operators, lotteries and gaming machines, and casinos) and non-profit organizations. Among the areas most exposed to the risk of financing of terrorism are consumer credit, the non-profit sector and the art market. A high level of risk is also attached to the use of cash, especially in relation to the trading of high-value goods. Areas of vulnerability and safeguards common to all sectors are also identified; these include transparency in the beneficial ownership of companies and trusts, supervision of intermediaries in cross-border contexts and cooperation between FIUs.

The mitigation measures required are specifically addressed by the Fifth Directive (completing the risk-based approach, setting up registers to identify beneficial ownership and strengthening cooperation between FIUs); others will have to be introduced through new provisions or policy initiatives.

As envisaged by the Fourth Directive,[10] the Report contains Recommendations from the Commission with which Member States are requested to comply according to the 'comply or explain' principle, and which aim to address and reduce the risk factors identified.

The Recommendations cover the following aspects: a) national Risk Assessments must specifically take into consideration the threats and vulnerabilities set out in the supranational assessment; b) the scope of the obliged entities must be defined by taking account of risks and, where necessary, it must go beyond the minimum as defined in the Directive; c) AML supervision must be increased, above all through inspections; d) customer due diligence must be stepped up to take account of sectors or activities exposed to greater risks; e) the supervisory authorities and the FIUs need more resources; f) effective national measures for the transparency of beneficial ownership are urgently required; and g) updated guidelines are needed for the various categories of obliged entities.

Together with the Supranational Risk Assessment, the Commission published a policy document entitled 'On Improving Cooperation between EU Financial Intelligence Units' entirely dedicated to building on the results of the Mapping Exercise by identifying priority areas for intervention.

[10] Article 6(4).

1.3. National legislation

1.3.1 Provisions on anti-money laundering and combating the financing of terrorism

On 4 July, Legislative Decree 90/2017 came into force, which modified Legislative Decree 231/2007 in order to transpose the Fourth Directive on anti-money laundering and terrorist financing.[11] Amendments were also made to Legislative Decree 109/2007 with specific reference to combating the financing of terrorism.

The reform – the main aspects of which, in relation to the approval procedure and the contents, were illustrated in the UIF's Annual Report of May 2017[12] – confirms the institutional framework of the existing prevention system and contains various innovations regarding the list of obliged entities, cooperation between authorities, the anti-money laundering obligations subject to a broader application of the risk-based approach and to simplification, and the sanctions system.

In this context, new regulatory powers are envisaged for the UIF for the detection and reporting of suspicious transactions; the forms of institutional cooperation and the information sources for financial analysis, together with the analysis of phenomena, of types of money laundering or of terrorist financing have also been expanded.

Following the entry into force of the reform, the competent authorities have been engaged in applying the new measures, disseminating guidelines and implementing the first regulatory interventions.

The UIF's indications

On 4 July 2017, the UIF also published a Notice providing the obliged entities with indications for confirming and updating the measures on active cooperation and aggregate AML reports.

The Unit made it particularly clear that the measures regarding the following remain applicable: the data and information to be included in STRs; those concerning aggregate AML reports; the anomaly indicators issued for all obliged entities (other than general government offices); anomalous behaviour models and patterns; and the Unit's Notices on operations at risk (preventing the financing of terrorism, anomalous use of virtual currencies and payment cards). Lastly, it stated that obliged entities no longer have to send the UIF communications of transactions to return funds in accordance with the Measures issued by the Unit on 6 August 2013 and 10 March 2014.

Clarifications from the other authorities

The Ministry of Economy and Finance (MEF) made a list of updated FAQs on the new decree available on its website.[13]

In its Circular of 7 July 2017, the General Command of the Finance Police reviewed the main innovations regarding anti-money laundering, the financing of terrorism and cash-for-gold, and set out the preliminary directives for its operating units.

On 9 February 2018, the Bank of Italy provided supervised intermediaries with

[11] The authorization for the Government and the relative criteria are contained in Law 170/2016, European Delegation Bill 2015.
[12] See Annual Report of the UIF on activities carried out in 2016, Section 1.1.
[13] See http://www.dt.tesoro.it/it/faq/faq_prevenzione_reati_finanziari.html.

indications as to which implementing provisions in the existing rules are still applicable; observing these indications ensures compliance with the new legislative framework even after the transition period has expired.

On 28 March, IVASS issued something similar for insurance companies and intermediaries.

The Protocol with the DNA

Among the initiatives to implement the reform, the Protocol signed on 5 October 2017 between the UIF, the National Anti-Mafia Directorate (DNA), the Finance Police and the State Police Department is particularly important, pursuant to the new provisions governing information exchanges with the DNA.[14]

The Protocol envisages the matching between the personal data of the subjects included in the STRs (rendered anonymous thanks to specific encryption techniques) and those in the database available to the DNA. By means of this matching, the DNA can detect: the relevance of the data to court cases, with the subsequent involvement of the competent public prosecutors, or the presence of names in its databases; in this case, where reasons of specific interest recur, the DNA can ask the UIF for all the information or analyses needed for investigations. The DNA gives the UIF feedback on the usefulness of the information received.

On 7 May 2018 a bilateral Protocol was signed between the DNA and UIF, which sets out the technical and operational aspects of their cooperation.

Feedback

The new regulatory framework enhances the two-way nature of the Unit's information exchanges with the investigative authorities by increasing the feedback on the investigative results of STRs.[15] On the basis of this feedback flow, the UIF will send its own feedback to reporting entities; this was limited to dismissed reports in the previous regulatory framework.

Access to investigative data

The investigative authorities are currently analysing some applicative issues for the implementation of the new decree's measures requiring the UIF to be provided with the investigative information necessary for financial analysis and for cooperation with the foreign FIUs.[16]

Instructions for general government offices

The UIF drew up instructions and indicators for the general government offices, which are no longer included among the obliged entities but are obliged to report any data and information concerning suspicious transactions to the Unit. In its meeting of 27 March 2018, the Financial Security Committee (FSC) gave a favourable opinion on the Unit's measure and also approved the guidelines for the mapping and assessment of risks by the general government entities concerned.[17]

The UIF's instructions govern the prerequisites, method and content for communicating data and information on suspicious transactions, and establish that general government entities must nominate a manager to assess and send communications to the Unit. The anomaly indicators are designed to reduce the margins of uncertainty in subjective assessments linked to STRs and to contribute to limiting costs and to the correctness and uniformity of the reports. The indicators relate

[14] Article 8 of Legislative Decree 231/2007.
[15] Article 41 of Legislative Decree 231/2007.
[16] Article 12(4) and Article 13 of Legislative Decree 231/2007.
[17] Article 10(1) of Legislative Decree 231/2007.

to the identity or behaviour of the subject involved in the transaction and to how the transaction was requested or carried out; they also take account of the specificities of the sectors of activity (public tenders and contracts, public funding, real estate and trade).

The FSC's guidelines reiterate the applicative part of Article 10 of the anti-money laundering decree and describe the role of general government in the AML system. The abovementioned guidelines establish that general government offices should proceed with the mapping of money laundering and financing of terrorism risks, and adopt internal procedures suitable for assessing, managing and mitigating risks, retrieving data and information on suspicious transactions and sending them promptly to the UIF, and ensuring maximum confidentiality for the subjects mentioned in the report and standardized conduct.

Threshold-based communications

One significant innovation introduced by the reform concerns the threshold-based communications that obliged entities must periodically send to the UIF and that refer to data and information identified on the basis of objective criteria linked to money laundering or terrorist financing risks.[18] The Unit will use this new kind of communication to analyse suspicious transactions and phenomena and typologies of interest. The relative rules will be issued by the UIF, after consultation with the FSC. Initially, these communications will deal with cash transactions for amounts above a given threshold and will be required from banks, payment institutions and e-money institutions. The Unit's instructions will provide indications in the event that sending a threshold-based communication excludes the obligation to report suspicious transactions.

MEF draft decree on exchangers and other virtual currency operators

Legislative Decree 90/2017, partly in anticipation of the new provisions in the Fifth European Directive, also lists virtual currency service providers among the obliged entities, but only as regards the conversion between virtual currencies and currencies that have legal tender.[19] In this context, from 2 to 16 February 2018, the Ministry of Economy and Finance submitted a draft decree for the initial recognition of the said service providers for public consultation, also for the purpose of including them in the register maintained by the Organization of Agents and Mediators (Organismo degli Agenti e dei Mediatori - OAM).[20]

This decree envisages the obligation to communicate to the Ministry the intention to operate as a virtual currency service provider in Italy, which also applies to 'operators that accept virtual currencies as payment for the provision of goods, services or other utilities'. In relation to this text, the Unit emphasized the need to specifically identify the operators that carry out the conversion of virtual currencies, since the new regulatory framework requires them to fulfil anti-money laundering obligations.

Register for gaming distributors and operators

As part of the provisions for gaming service providers, in December 2017 a register for gaming distributors and operators was set up with the Customs and Monopolies Agency.[21]

---

[18] Article 47 of Legislative Decree 231/2007.
[19] Article 3(5)(i), of Legislative Decree 231/2007.
[20] Article 17-bis of Legislative Decree 141/2010, as amended by Legislative Decree 90/2017.
[21] Article 52-bis of Legislative Decree 231/2007, introduced by Law 205/2017, relative to the 'National budget for the financial year 2018 and the multi-annual budget for the three-year period 2018-2020'.

The register records identifying data for distributors and operators, and cases where contractual relations have ceased with operators owing to non-fulfilment of requirements or to serious or repeated infringements found during inspections, or to the suspension of activities by the MEF as a result of checks by the Finance Police. The MEF, the UIF, the Finance Police, the Anti-Mafia Investigation Department (DIA) and the DNA can all access the register, as can police headquarters and gaming licensees.

The supervisory authorities' provisions

In order to implement the new primary legislation, the sectoral supervisory authorities drew up draft measures, applicable to supervised entities, which were submitted for consultation in April and May 2018.

Bank of Italy

The Bank of Italy, together with the UIF, prepared supervisory measures for intermediaries regarding organization, procedures and internal controls, and customer due diligence. Work is under way to define the provisions for conserving data.

The main changes in the provisions for organization, procedures and internal controls refer to: the methodology for risk self-assessment, the central contact point, and reporting suspicious transactions. The provisions for central contact points implement those of the decree which include EU intermediaries that use one or more agents and accredited entities among the obliged entities; the contact point represents the intermediary in Italy and is the sole interlocutor with the authorities, which makes it possible to remedy the fragmentation of the foreign operators' distribution network; this is supervised by the Bank of Italy. With regard to active cooperation, the following measures aim to: regulate the appointment of and requirements for managers or officers responsible for reporting suspicious transactions; enhance their role, which also involves assessing suspicious transactions that they know about in the absence of any communication arising from first-level company checks and carrying out sample checks to verify their adequacy; establish the importance of reporting for updating customers' risk profiles; strengthen the safeguards for the confidentiality of all subjects involved in reporting procedures; and increase the synergies and effectiveness of reporting within group structures. Other provisions clarify and update the existing measure and expand some solutions already included in the rules on internal controls for banks to all the intermediaries. The joint guidelines of the European supervisory authorities have been transposed regarding the information to be included in the messages accompanying transfers of funds.

Similarly, the provisions for customer due diligence take account of the changes made. The most important aspect of the rules is the maximization of the risk-based approach, which guides the methods and the extent of the analyses carried out by intermediaries as part of their 'know your customer' activities. There are also new provisions regarding beneficial owners, for whom additional indications to those provided for by law are given, such as the identification of remote checking instruments and the possibility to make use of customer due diligence via third parties even when the latter have done so remotely.

Consob and IVASS

Consob has drawn up provisions for organization, procedures and internal controls, customer due diligence and data conservation for supervised auditors and auditing firms. Clarifications on the transition regime applicable to the same subjects in the new regulatory framework were provided during the consultation.

IVASS has compiled a single document for the rules on organization, procedures and internal controls and customer due diligence for insurance companies and

intermediaries.

The rules contain the updates, additions and specifications needed in light of the new legislation and of the results of supervisory activity, so as to strengthen the safeguards and give more room to the risk-based approach.

Initiatives of self-regulatory bodies and industry associations

The new context emphasizes the role of the self-regulatory bodies for the professions that are given the task of drawing up technical rules for risk analysis procedures and methodologies, internal controls, customer due diligence and record-keeping requirements.[22]

The CNN, the CNF and the CNDCEC have prepared drafts of technical rules for the areas indicated by the decree, and discussions are under way at the MEF, in which the UIF and the Finance Police are also taking part, in view of the rules being submitted to the FSC for the issuance of an opinion as envisaged by law.

In a meeting on 27 March 2018, the FSC approved a methodology to support the activity of self-regulatory entities in order to facilitate the mapping and rating of money laundering and financing of terrorism risks.

As regards the model already tested with representatives of transport and safe custody service operators, the Unit has responded to the UNIREC's request for an opinion on possible explanations about anti-money laundering for their associates.

Sanctions for failure to report suspicious transactions

Legislative Decree 90/2017 has significantly altered the regulations on money laundering sanctions, setting out a comprehensive system of cases and areas of competence. The innovations regarding violations of the obligations to report suspicious transactions include those for the classification (in terms of seriousness, systematic nature or repetition) and level of responsibility for the violation; on the basis of this classification, sanctioning powers are assigned to the supervisory authorities (Bank of Italy, Consob and IVASS) for legal persons and to the Ministry of Economy and Finance for natural persons (staff and those holding positions in administration, management and control).

The UIF swiftly adapted its operational procedures for ascertaining and contesting violations of reporting obligations to the new sanctions framework. Specifically, these procedures – drawn up in cooperation with the supervisory authorities and the Ministry of Economy and Finance – deal with: the classification of failure to report a suspicious transaction in terms of seriousness, systematic nature and repetition; the contesting of the facts to be ascertained regarding non-supervised obliged entities and staff from the intermediaries and trust companies, or the sending of documents to the supervisory authorities for assessing the possible level of responsibility for supervised entities; and the application of the 'favor rei' envisaged by the legislation for the transition period to the new rules.[23]

MEF Circular on sanctions

As regards sanctions, the MEF's Circular of 6 July 2017 is also important as it provides operational indications for the department's competent central and territorial offices. With respect to the failure to report suspicious transactions, a 'serious' breach is distinguished from an 'ordinary' breach because of the 'serious', 'repeated', 'systematic'

[22] Article 11 of Legislative Decree 231/2007.
[23] Article 69 of Legislative Decree 231/2007.

or 'multiple' nature of the violation, to be ascertained following the criteria set out in the anti-money laundering decree and in the Circular.

The Bank of Italy's sanction provisions

In relation to the sanctioning competences developed in the field of anti-money laundering, the Bank of Italy – assisted by the UIF – prepared a consultation paper containing the new provisions on administrative sanction proceedings. The rules are intended for supervised obliged entities and, in compliance with the legal requirements for violations other than failure to report suspicious transactions, for those holding positions in administration, management and control. The sanction procedure is governed from the investigation of the violation to the adoption, notification and publication of the measure.

As part of the reform to rationalize and make criminal law more widely-known, the crime of misusing and falsifying credit and payment cards previously contained in the AML decree has been transferred to the penal code.[24]

Notice on 'returnees'

With regard to the fight against the financing of terrorism, in view of the growing threat and risk of inflows to western countries of returnee terrorists, on 13 October 2017 the UIF issued a Notice to upgrade the capacity of those with active cooperation obligations to intercept suspicious elements traceable to such events.[25]

1.3.2. Other regulatory measures

The Anti-Mafia Code

The legislature has made changes to the Anti-Mafia legislation and to other provisions in force regarding personal and asset protection measures, administration, the management and destination of goods, the third-party protection system and relations with bankruptcy procedures, the administrative liability of entities and extended confiscation.[26]

With reference to the Anti-Mafia Code, the main changes are as follows: (i) the list of entities subject to preventive measures has been extended to include: those suspected of assisting associates,and of terrorist offences; those carrying out preparatory or executive acts to subvert state law, or committing crimes for terrorist purposes, also at international level, or taking part in a conflict abroad to support an organization that pursues terrorist objectives; those suspected of conspiring to commit various offences against general government, of aggravated fraud to obtain public funds and of stalking; (ii) changes have been made to the seizure or confiscation of an equivalent value; (iii) there are new rules to guarantee transparency and a rotation in the choice of judicial administrators; (iv) the tasks assigned to the national agency for confiscated assets have been extended; (v) the judicial control of firms has been regulated; (vi) it is envisaged that confiscation shall in no way affect the rights of third parties to make claims or any security interests established prior to the seizure, provided that certain conditions are met; in this regard it has been established that 'the decree under which the application for admission of a claim has been conclusively rejected, pursuant to Article 58(2), due to the non-recognition of good faith in granting the claim, proposed by a subject under

[24] See Legislative Decree 21/2018, which introduced Article 493-ter of the penal code and revoked Article 55(5) and (6) second paragraph of Legislative Decree 231/2007.
[25] See Section 5.2.
[26] This refers to Law 161/2017 which amended Legislative Decree 159/2011.

Bank of Italy supervision, shall be communicated to the latter under Article 9 of Legislative Decree 231/2007, as amended'.[27]

The 2016-2017 European Delegation Bill

In accordance with the 2016-2017 European Delegation Bill,[28] the Government approved the outline of the legislative decree[29] to transpose the Directive on access by the tax authorities to anti-money laundering information into national law.[30]

The new European rules amend the previous Directive,[31] establishing that EU Member States must allow the tax authorities to access information on customer due diligence, the beneficial ownership of entities, companies and trust companies, and data storage, in order to fight more effectively against tax evasion and fraud.

The 2016-2017 European Delegation Bill also contains the authorization for the Government for the transposition of the Directive on personal data processing[32] by the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and for the free movement of such data at European level, and of the Directive on the fight against terrorism,[33] which establishes minimum harmonization rules for defining terrorist offences and the relative sanctions.

The law on whistleblowing

The law on whistleblowing[34] sets out provisions for protecting persons disclosing crimes or irregularities witnessed as part of a public or private working relationship; it prohibits discriminatory acts against whistle-blowers for reasons linked to the reported facts and it ensures the confidentiality of their identity. The whistle-blower or the unions can notify the National Anti-Corruption Authority (ANAC) of any retaliatory measures taken, which then has the right to exercise its sanctioning powers.[35]

The new rules extend protection to whistleblowing in the private sector[36] and introduce an exemption from the obligation of professional, business, scientific and industrial secrecy, justified by the pursuit of the interest of the integrity of administrations, and the prevention and repression of misappropriations.

The decree transposing PSD 2

The legislature[37] transposed the Directive relating to payment services in the domestic market[38] (PSD2 – Payment Services Directive), which promotes the development of a single European market for payment systems, at the same time strengthening the safeguards for users and the security of electronic payments. This includes the rules for compliance with the Regulation on interchange fees for card-based payments.[39]

---

[27] Article 52(3-bis) of the Consolidated Law on Finance. 159/2011, introduced by Legislative Decree161/2017.
[28] Law 163/2017.
[29] Government Act No. 504.
[30] Directive (EU) 2016/2258.
[31] Directive (EU) 2011/16.
[32] Directive (EU) 2016/680, transposed by Legislative Decree 51/2018.
[33] Directive (EU) 2017/541.
[34] Law 179/2017.
[35] Article 54-bis of Legislative Decree 165/2001.
[36] Article 6 of Legislative Decree 231/2001, as amended by Law 179/2017.
[37] Legislative Decree 218/2017.
[38] Directive (EU) 2015/2366.
[39] EU Regulation 751/2015.

The negative scope, i.e. exemptions to which the decree does not apply, has been revised. The changes made also concern payments made: (i) through a commercial agent 'provided that they act only on behalf of the payer or the payee or if the agent never enters into possession of the customer's funds'; (ii) with instruments that can only be used in a limited way and that meet certain conditions; and (iii) using mobile phone credit, provided that the payment transaction does not exceed certain limits (€50 for each transaction and €300 per month for the cumulative value of payment transactions) and responds to the purposes laid down by the law.

The rules identify two new payment services: 1) the payment initiation service, which consists of a payment order requested by a payer to be debited from an account held with another payment service provider; and 2) the account information service which is the online service providing information about one or more payment accounts held by the payer with one or more payment service providers.

As regards the activities identified by the decree, there are new players who are in any case included among payment service providers: (i) Card Based Payment Instrument Issuers authorized to issue card-based payment instruments, who will be able to ask the payment service provider holding the account to confirm that there are sufficient funds to cover the payment (fund checking); (ii) payment order service providers; and (iii) account information service providers.

With reference to money remittances, it is specified that this service refers to the transfer of an amount 'expressed in legal tender'. It introduces the concept of 'strong customer authentication', which the payment service provider must apply when the payer accesses their online payment account, makes an electronic payment or does anything that may imply a risk of payment fraud.

The rules on payment services envisage that payment service providers operating in Italy through agents and without a branch, pursuant to Article 128-quater of the TUB, shall designate a central contact point in Italy in the cases of and for carrying out the duties envisaged by the regulatory technical standards issued by the European Commission in accordance with the PSD2, according to the provisions set out by the Bank of Italy. There are no changes to the current provisions regarding contact points, accredited entities and agents for combating money laundering and the financing of terrorism.[40]

The 'cash-for-gold shops' decree

On 5 July 2017 the decree on 'cash-for-gold shops' came into force,[41] which sets out provisions to guarantee the full traceability of trading in used precious items and to prevent this market from being used for illegal purposes.

The decree obliges cash-for-gold businesses to identify their customers, store data and report suspicious transactions to the UIF; it provides for the use of a current account exclusively for this activity and for means of payment other than cash for amounts equal to or more than €500, in order to guarantee the complete traceability of transactions to their participants. Violations are punished with administrative fines imposed by the Ministry of Economy and Finance.

[40] Article 128-decies of the TUB (Consolidated Law on Banking).
[41] Legislative Decree 92/2017.

Cash-for-gold business is only for operators holding a licence under Article 127 of the TULPS (Consolidated Law on Public Security), who must apply for inclusion in a special register managed by the OAM. How to send the data and have it entered in the register will be established by a specific MEF decree. Running a cash-for-gold business without being included in the register is unlawful and punishable under criminal law.[42]

MEF Decree on tax matters

The Ministry of Economy and Finance updated the list of countries that make possible an adequate exchange of information on tax matters in a decree to this effect,[43] adding the following countries: Andorra, Barbados, Chile, the Holy See, Monaco, Nauru, Niue, Saint Kitts and Nevis, Saint Vincent and the Grenadines, Samoa and Uruguay.

Investor Visa Committee for Italy

The Decree of 21 July 2017, issued by the Ministry of Economic Development together with the Ministry of Foreign Affairs and International Cooperation and the Ministry of the Interior, includes the UIF among the authorities competent to assess the compliance of visa applications from foreigners intending to make investments or charitable donations for significant amounts in Italy (Investor Visa Committee for Italy).[44]

[42] Article 8 of Legislative Decree 92/2017.
[43] MEF Decree of 23 March 2017 which updates the previous Decree of 4 September 1996.
[44] See Section 8.3.

2. ACTIVE COOPERATION

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

Centralizing the flow of information at the Unit means that the evaluations can be standardized and integrated in order to identify subjective and objective links, trace financial flows even beyond Italy's borders, reconstruct innovative ways to launder money and select those cases with a higher level of risk.

The Unit sends the results of its analyses to the competent law enforcement bodies (the NSPV - Special Foreign Exchange Unit of the Finance Police and the DIA - the Anti-Mafia Investigation Department) for further investigation. The suspicious transaction reports are sent to the judicial authorities if crimes are involved or if the authorities themselves request the reports. The results of the analysis may be sent to the supervisory authorities if important cases are detected.

The Unit uses this vast body of information to develop anomaly indicators and identify patterns of anomalous behaviour to guide reporting entities in detecting suspicious transactions.

2.1. Reporting flows

In 2017 the UIF received 93,820 reports,[45] about 7,200 fewer than in 2016 (-7.2 per cent) (see Table 2.1).

Table 2.1

Reports received

	2013	2014	2015	2016	2017
Number of reports	64,601	71,758	82,428	101,065	93,820
Percentage change on previous year	*-3.6*	*11.1*	*14.9*	*22.6*	*-7.2*

The decrease in the overall reporting is attributable to the fading of the effects of the voluntary disclosure measures to regularize funds held abroad,[46] which had led to the marked increase of 2016. Net of those cases attributable to such measures, the

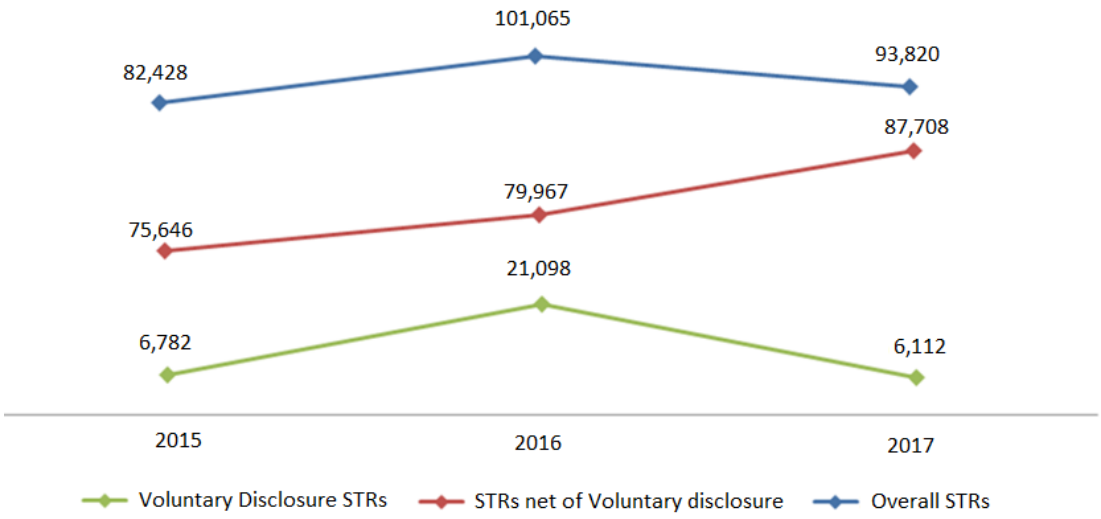
[45] Detailed information on suspicious transaction reports can be found in the *Quaderni dell'antiriciclaggio, Collana Dati statistici*, published on the UIF's website.

[46] This refers to both the voluntary disclosure introduced by Law 186/2014, and to the voluntary disclosure bis, provided for in Legislative Decree 193/2016, converted with amendments into Law 255/2016.

reports sent overall in 2017 by obliged entities have not only increased, but have recorded the highest growth rate of the last three years; 9.7 per cent against 5.7 per cent in 2016 and 5.4 per cent in 2015 (see Figure 2.1).

Figure 2.1

Reporting flow: percentage of Voluntary Disclosure[1]



[1] The data include reports classified by reporting entities as being related to the voluntary disclosure category, as well as those classified as such by the UIF during their processing.

Before analysing this flow of reports in detail, it is important to point out that, in redefining the range of obliged entities, the new anti-money laundering decree has made some changes to the previous classifications. The macro-categories shown below therefore reflect the structure established by the law; the new classifications have also been adopted for the data relating to 2016, making it easier to compare them with this year's data.

As in the past, the highest number of reports received (77 per cent of the total) came from the 'Banks and Poste Italiane SpA' category (which from now on will simply be referred to as the 'banks' category) although with a decrease of 8 per cent compared with 2016. The increase in STRs from other intermediaries and financial operators continues, confirming it as the second macro-category of obliged entities as regards the number of reports sent, with an increase of about 19 per cent. There has also been an increase compared with 2016 for non-financial operators and gambling service providers[47] (+25 per cent on average). The reports sent by general government[48]

[47] The new version of Legislative Decree 231/2007, as regards the list of obliged entities in accordance with Article 3, separates non-financial operators (paragraph 5) from gaming service providers (paragraph 6), which were previously in the same category.

[48] As of 4 July 2017, general government is no longer part of the obliged entities, as it is not included in Article 3 of Legislative Decree 231/2007, as amended by Legislative Decree 90/2017. The new rules, listed in Article 10(4) of the abovementioned decree, provide that 'in order to enable financial analyses to be made, aimed at uncovering recycling and financing of terrorism activities, general government communicates to the UIF any data or information concerning suspicious transactions that come to its attention in the course of its institutional activities (...)'. See Section 1.3.1.

recorded a marked increase in percentage terms, though were still extremely low in terms of figures: 70 reports compared with 10 in 2016 (see Table 2.2).

Table 2.2

STRs by type of reporting entity

	2016		2017		
	(absolute values)	*(% share)*	*(absolute values)*	*(% share)*	*(% change on 2016)*
Total	**101,065**	**100.0**	**93,820**	**100.0**	**-7.2**
Banks and Poste Italiane SpA	78,418	77.7	72,171	76.9	-8.0
Financial intermediaries excl. Banks and Poste Italiane SpA	11,250	11.1	13,347	14.3	18.6
Companies managing markets and financial instruments	1	0.0	5	0.0	400.0
Professionals	8,801	8.7	4,969	5.3	-43.5
Non-financial operators	535	0.5	658	0.7	23.0
Gaming service providers	2,050	2.0	2,600	2.8	26.8
General government offices	10	0.0	70	0.0	600.0

Financial intermediaries other than banks

With regard to financial operators other than banks, the contribution from Electronic Money Institutions and from EU points of contact is noteworthy, as their reports more than quadrupled, from 328 in 2016 to 1,444 in 2017. This flow is heavily concentrated, with 93 per cent of the reports coming from just one of the five operators in the category, as was also the case in 2016, although the overall figures were much lower. In order of percentage increase, the next categories are insurance companies (+24.5 per cent) and the group comprising asset management companies, SICAVs and SICAFs (+24.2 per cent). The contribution from payment institutions and the relative points of contact also rose, from 5,643 reports in 2016 to 6,575 in 2017: money transfer operators play a leading role in this group, with 5,224 reports accounting for almost 80 per cent of the total for this category.[49]

One of the most significant negative changes was recorded by investment firms, with a decrease of over 75 per cent. There was also a significant decline for trust companies - Article 106 of the 1993 Banking Law – of -21.8 per cent, also caused by the fall in the number of reports connected with the voluntary disclosure procedures: the share of STRs linked to this phenomenon fell drastically, standing at 19.5 per cent of the total, against the figure of 76 per cent recorded in 2016 (see Tables 2.3 and 2.5).

[49] Some 92 per cent of these reports were sent by the leading four operators in the sector.

Table 2.3

STRs by category of banking and financial intermediary

	2016		2017		
	(absolute values)	*(% share)*	*(absolute values)*	*(% share)*	*(% change on 2016)*
Banks, intermediaries and other financial operators	**89,668**	**100.0**	**85,518**	**100.0**	**-4.6**
Banks and Poste Italiane SpA	**78,418**	**87.5**	**72,171**	**84.4**	**-8.0**
Financial intermediaries excl. Banks and Poste Italiane SpA	**11,250**	**12.5**	**13,347**	**15.6**	**18.6**
Payment Institutions and contact points of EU payment service providers	5,643	6.3	6,575	7.7	16.5
Insurance companies	2,185	2.4	2,721	3.2	24.5
Electronic Money Institutions and contact points of EU Electronic Money Institutions	328	0.3	1,444	1.7	340.2
Trust companies - Article 106 of the 1993 Banking Law	1,348	1.5	1,054	1.2	-21.8
Financial intermediaries - Article 106 of the 1993 Banking Law [1]	794	0.9	781	0.9	-1.6
Asset management companies, SICAVs and SICAFs	265	0.3	329	0.4	24.2
Investment firms	252	0.3	62	0.1	-75.4
Intermediaries and other financial operators not included in the previous categories [2]	435	0.5	381	0.4	-12.4

[1]Articles 106 and 107 of Legislative Decree 385/1993, prior to the reform contained in Legislative Decree 141/2010 which eliminated the general and special registers envisaged by Articles 106 and 107 and instituted the new register pursuant to Article 106 of the TUB.

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

Professionals

The significant reduction in the figure for professionals (-44 per cent) seems broadly attributable to the role they played, especially in the activation of the voluntary disclosure procedure, whose repercussions on STRs declined markedly in 2017, as mentioned previously More in detail, in descending order, the reports submitted decreased from law firms, law and accounting firms and law practices (-93.4 per cent), accountants, bookkeepers and employment consultants (-72.8 per cent), and lawyers (-76.2 per cent). In contrast, there was an increase in the contribution from auditing firms and auditors (+18 per cent), as well as from notaries and from the CNN, with the latter's reports going up from 3,582 to 4,222, an increase of nearly 18 per cent. The CNN continued to play an important role in 2017 too, sending almost 98 per cent of the reports from its category. The same has not yet occurred with reference to the National Council of the Order of Accountants and Bookkeepers (CNDCEC), which forwarded 147 of the total of 361 reports sent overall by this category.

This is probably attributable to the fact that the memorandum of understanding[50] between the UIF and the category's National Council was only recently drawn up (signed in December 2016 but in effect since May 2017, when the first report was forwarded by the CNDCEC), and it is likely that the number of their reports will gradually increase.

Non-financial operators

The number of reports from non-financial operators increased, specifically from gold traders and manufacturers and retailers of precious stones and metals (251 against 55 in 2016) and from cash-in-transit and valuable items transport companies: the latter, included in the other non-financial operators' category, sent 388 reports. The growth rate for gaming service providers continued to be significant (around +27 per cent compared with 2016), albeit less so than in the past (there was an increase of almost 40 per cent between 2015 and 2016; see Table 2.4).

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

Table 2.4

STRs received from professionals and non-financial operators					
	2016		2017		
	(absolute values)	*(% share)*	*(absolute values)*	*(% share)*	*(% change on 2016)*
Non-financial obliged entities	**11,386**	**100**	**8,227**	**100**	**-27.7**
Professionals	**8,801**	**77.3**	**4,969**	**60.4**	**-43.5**
Notaries and National Council of Notaries	3,582	31.5	4,222	51.3	17.9
Law firms, law and accounting firms and law practices	3,388	29.8	222	2.7	-93.4
Accountants, bookkeepers and employment consultants	1,326	11.6	361	4.4	-72.8
Lawyers	424	3.7	101	1.2	-76.2
Auditing firms, auditors	22	0.2	26	0.3	18.2
Other professional services providers[1]	59	0.5	37	0.5	-37.3
Non-financial operators	**535**	**4.7**	**658**	**8.0**	**23.0**
Gold traders and manufacturers and retailers of precious stones and metals	55	0.5	251	3.1	356.4
Antique dealers and auction houses	0	0.0	1	0.0	NA
Other non-financial operators[2]	480	4.2	406	4.9	-15.4
Gaming service providers	**2,050**	**18.0**	**2,600**	**31.6**	**26.8**

[1] The category includes the entities listed in Article 3(4) letter (b)
[2] The category includes the other entities listed in Article 3(5) letter (b) of Legislative Decree 231/2007, as amended by Legislative Decree 90/2017, not included in the previous categories.

The impact of voluntary disclosure

As has already been pointed out, the decline in STRs linked to voluntary disclosure was the main reason for the fall in the number of incoming STRs. Reports of this kind[51] went down from 21,098 in 2016 to 6,112 in 2017, a figure that is also lower

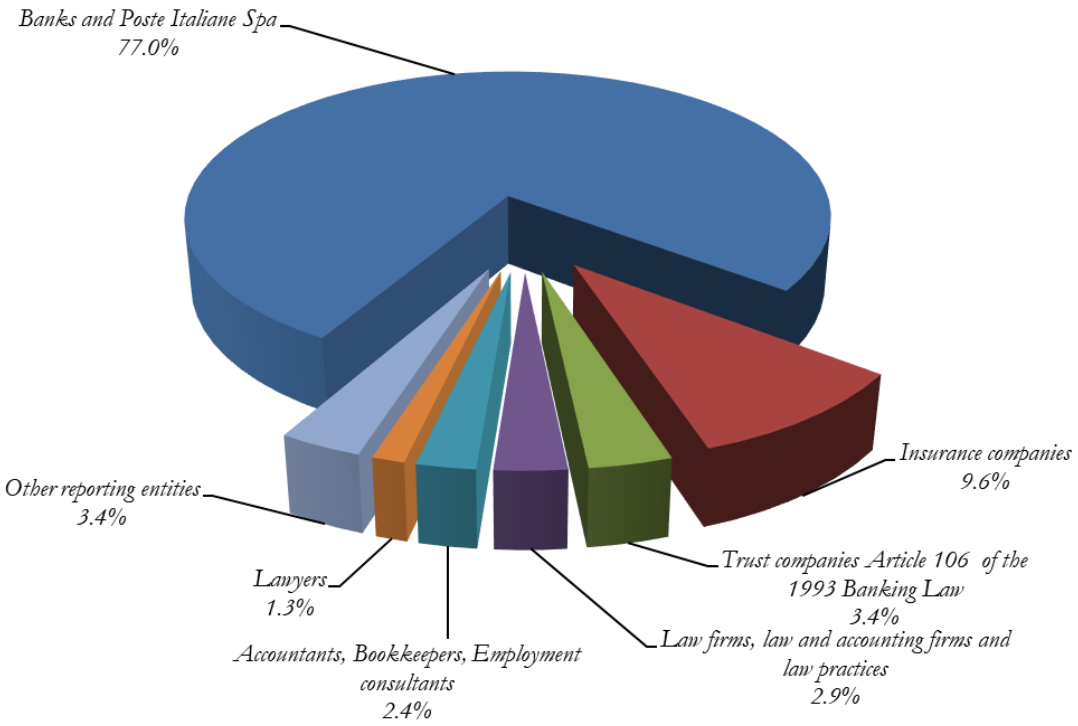
[51] The data include reports classified by reporting entities as being related to the voluntary disclosure category, as well as those classified as such by the UIF during their processing.

than that recorded in 2015 (6,782), the first year affected by this phenomenon. These reports accounted for 6.5 per cent of the total against 21 per cent in 2016 and 8 per cent in 2015.

As regards the percentage share of the various reporting categories for this type of STR, the contribution from banks increased (by more than 10 percentage points compared with the previous year) as did that from insurance companies (+6.7 percentage points). The share of reports from accountants, bookkeepers and employment consultants fell to 2.4 per cent of the total for this category, against 5.7 per cent in 2016 and 20 per cent in 2015. These changes can reasonably be attributed to the different role played by each of these categories in the various phases of regularization: initial activation of the procedure (accountants), and the subsequent repatriation of funds (banks and insurance companies). (See Figure 2.2 and Table 2.5).

Figure 2.2

Distribution of voluntary disclosure STRs by type of reporting entity



The category 'Other reporting entities' includes notaries and the National Council of Notaries, asset management companies, SICAVs and SICAFs, investment firms, Electronic Money Institutions and the related points of contact, trust companies under Law 1966/1939 and general government.

Table 2.5

Reports connected to voluntary disclosure by type of reporting entity			
	Total STRs	**VD STRs [1]**	**%**
TOTAL	**93,820**	**6,112**	**6.5**
Banks and Poste Italiane SpA	**72,171**	**4,705**	**6.5**
Other financial operators	**13,347**	**943**	**7.1**
Payment Institutions and contact points of EU payment service providers	6,575	-	0.0
Insurance companies	2,721	589	21.6
Electronic Money Institutions and contact points of EU Electronic Money Institutions	1,444	1	0.1
Trust companies - Article 106 of the 1993 Banking Law	1,054	206	19.5
Financial intermediaries - Article 106 of the 1993 Banking Law	781	-	0.0
Asset management companies, SICAVs and SICAFs	329	51	15.5
Investment firms	62	15	24.2
Intermediaries and other financial operators not included in the previous categories	381	81	21.3
Companies managing markets and financial instruments	**5**	**-**	**0.0**
Professionals	**4,969**	**439**	**8.8**
Notaries and National Council of Notaries	4,222	29	0.7
Law firms, law and accounting firms and law practices	222	179	80.6
Accountants, bookkeepers and employment consultants	361	146	40.4
Lawyers	101	81	80.2
Auditing firms, auditors	26	-	0.0
Other professional services providers	37	4	10.8
Non-financial operators	**658**	**-**	**0.0**
Gold traders and manufacturers and retailers of precious stones and metals	251	-	0.0
Antique dealers and auction houses	1	-	0.0
Other non-financial operators	406	-	0.0
Gaming service providers	**2,600**	**-**	**0.0**
General government offices	**70**	**25**	**35.7**

[1] See footnote 51.

In 2017, 646 new entities registered with the system for reporting suspicious transactions, bringing the total to 5,779 at the end of the year. The new entities are mainly professionals (474), especially accountants and bookkeepers (328).

Of the new entities registered over the year, only 117 have actually submitted reports, with a total of 427 STRs; this seems indicative of the growing awareness of obliged entities regarding the fight against money laundering and the financing of terrorism, which encourages them to establish an initial contact with the Unit, registering even before there is any specific event to be reported.

As far as the new professionals registered are concerned, 89 have sent at least one report, for an overall total of 266 (of which 215 connected with money laundering, 50 with voluntary disclosure operations and 1 with financing of terrorism).

2.2. Suspicious transactions

The reports involving suspected money laundering continue to account for the majority of those submitted (92,824[52] out of a total of 93,820). There was a considerable increase in the number of reports relating to the suspected financing of terrorism, as a result of operators' growing awareness, given the exacerbation of the threats and the awareness-raising activities.[53] In terms of numbers, the reports relating to financing of terrorism amount to 981, against 619 in 2016, and also include those originally classified by reporting entities as belonging to the 'money laundering' category and later reclassified during the UIF's internal analysis process.

There were only 15 STRs on financing the proliferation of weapons of mass destruction (see Table 2.6 and Figure 2.3).

Table 2.6

Distribution of STRs by category

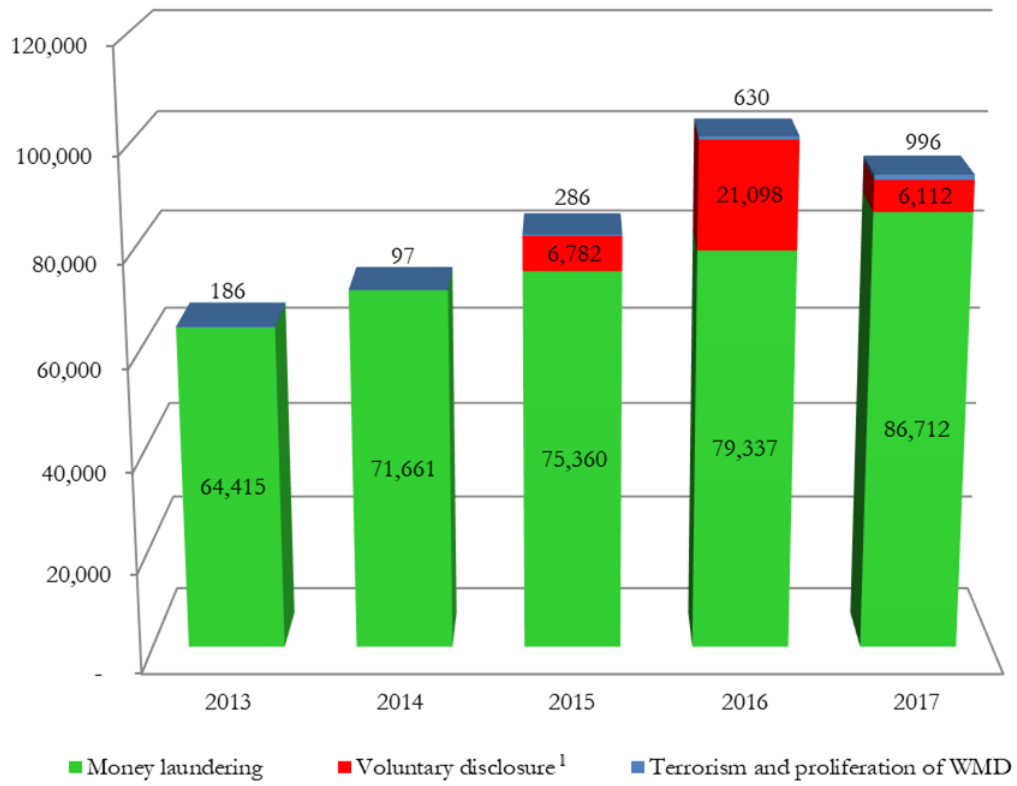
	2013	2014	2015	2016	2017
			(absolute values)		
Total	**64,601**	**71,758**	**82,428**	**101,065**	**93,820**
Money laundering	64,415	71,661	82,142	100,435	92,824
of which voluntary disclosure[1]			*6,782*	*21,098*	*6,112*
Financing of terrorism	131	93	273	619	981
Financing of proliferation of WMD	55	4	13	11	15

[1] See footnote 51.

[52] This data includes voluntary disclosure STRs, which constitute a subset of the broader category of money laundering.
[53] See Section 5.1.

Figure 2.3

Reports received
(*absolute values*)



[1] See footnote 51.

2018 Trends

In the first quarter of 2018, despite the sharp reduction in STRs connected with voluntary disclosure, the overall flow of reports remained similar to that of the previous year. The percentage distribution over the various categories changed, partly due to the increased number of reports sent by professionals, non-financial operators and gaming service providers.

The data for the first three months of 2018 confirm the growing trend in STRs connected with the financing of terrorism, with 337 reports of this kind submitted.

Territorial distribution of STRs

As regards the territorial distribution of STRs,[54] in 2017 Lombardy continued to be the leading region, despite a significant downturn compared with 2016 (-22.2 per cent); this seems to be attributable to the lower share of voluntary disclosure recorded in 2017, given that this region had made the largest contribution to the flow of reports in previous years. The other regions of northern Italy where, after Lombardy, voluntary disclosure had an impact, recorded negative shares in percentage terms (Emilia-Romagna -9.2 per cent, Piedmont -13.2 per cent and Liguria -0.1 per cent), except for Veneto, whose overall total rose by 4.3 per cent (see Table 2.7).

[54] Since more than one suspicious transaction can be included in each report, the source of the report is usually assumed to be the same as the place of the request/execution of the first transaction.

Table 2.7

Distribution of STRs received by region where transaction occurred

Regions	2016		2017		
	(absolute values)	*(% share)*	*(absolute values)*	*(% share)*	*(% change on 2016)*
Lombardy	25,373	25.1	19,744	21.0	-22.2
Campania	9,769	9.7	10,863	11.6	11.2
Lazio	9,325	9.2	9,435	10.1	1.2
Veneto	7,841	7.8	8,181	8.7	4.3
Emilia-Romagna	6,979	6.9	6,338	6.8	-9.2
Piedmont	7,100	7.0	6,165	6.6	-13.2
Tuscany	5,908	5.9	6,129	6.5	3.7
Sicily	4,497	4.4	5,003	5.3	11.3
Puglia	4,519	4.5	4,759	5.1	5.3
Liguria	2,911	2.9	2,908	3.1	-0.1
Calabria	2,127	2.1	2,657	2.8	24.9
Marche	2,067	2.0	2,059	2.2	-0.4
Friuli-Venezia Giulia	1,488	1.5	1,724	1.8	15.9
Abruzzo	1,265	1.3	1,464	1.6	15.7
Sardinia	1,153	1.1	1,265	1.3	9.7
Trentino-Alto Adige	1,099	1.1	1,210	1.3	10.1
Umbria	949	0.9	921	1.0	-3.0
Basilicata	521	0.5	529	0.6	1.5
Molise	316	0.3	315	0.3	-0.3
Valle d'Aosta	212	0.2	182	0.2	-14.2
Abroad[1]	5,646	5.6	1,969	2.1	-65.1
Total	**101,065**	**100**	**93,820**	**100.0**	**-7.2**

[1] The category includes reports from obliged Italian entities in which the required field 'Place of execution/Request' for the first transaction recorded has been filled in with a foreign country by the reporting entity. The foreign countries referred to most frequently are still Switzerland and the Principality of Monaco with 788 and 149 reports respectively, followed in third place by the United Kingdom with 95 STRs, a position held by San Marino in 2016. The significant decline (-65.1 per cent) in transactions reported by Italian intermediaries but classified under the 'Abroad' category is also due to fewer voluntary disclosure operations (793 reports).

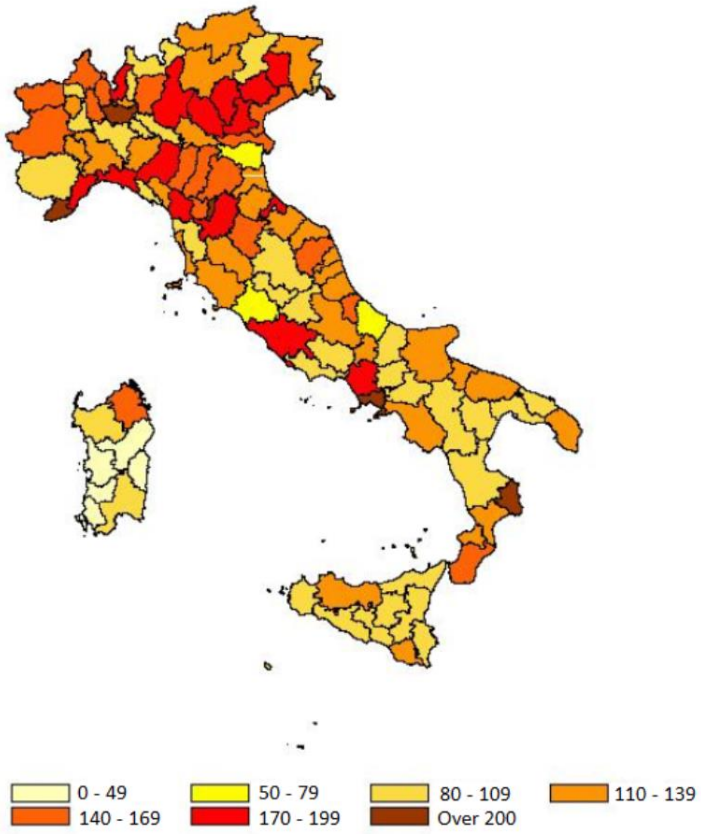
The ranking for the number of reports submitted remains essentially unchanged compared with 2016, except for Emilia Romagna which overtakes Piedmont, and Sicily which overtakes Puglia. The regions recording positive changes of more than 10 percentage points are, in descending order, Calabria (+24.9 per cent), Friuli-Venezia Giulia (+15.9 per cent), Abruzzo (+15.7 per cent), Sicily (+11.3 per cent), Campania (+11.2 per cent) and Trentino-Alto Adige (+10.1 per cent).

The values normalized on a provincial basis show that once again there was a high number of reports from the Milan area, followed by the provinces of Prato (in second place again), Imperia, Naples and Crotone, all in the highest class. They are followed in the ranking by five Sardinian provinces, which sent between 39 and 49 reports.

Figure 2.4

Distribution of STRs received by region where transaction occurred

(Number of STRs per 100,000 inhabitants)



Amounts reported

In 2017, the total value of suspicious transactions actually executed and reported to the UIF came to over €69 billion, against €88 billion in 2016.

Bearing in mind that both the transactions actually executed and those only attempted are reported, when the latter are also counted, the overall figure for 2017 exceeds €83 billion, although this is considerably lower than the previous year's figure of €154 billion. Generally speaking, estimates of the total value of the suspicious transactions reported must be treated with caution. It should be remembered that the system leaves to the discretion of each reporting entity the possibility of limiting the area of suspicion to a subset of the transactions structured in the STR overall. The calculation of the total value of the suspicious transactions is heavily influenced by the assessments of this kind made by the reporting entities. The same transaction may also be reported by more than one entity, leading to a multiplication of the amounts. This is an aspect that is even more important for voluntary disclosure reports, given the possible involvement of various reporting entities in the different steps of the

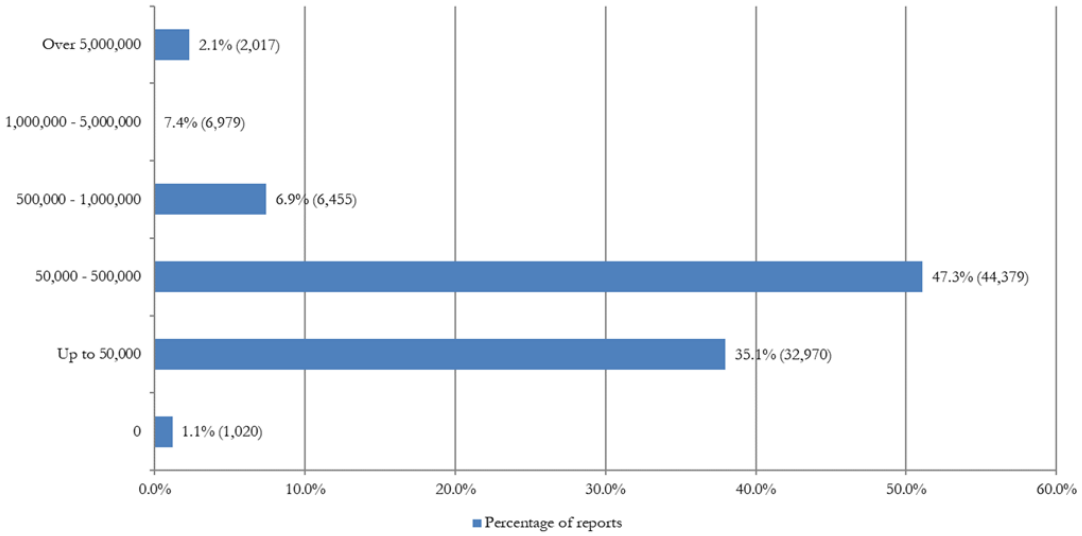
procedure; the considerable reduction in reports connected with voluntary disclosure measures, often in relation to transactions that are only planned and not actually made, seems to have played a significant role in limiting the amounts reported.

The distribution of STRs received by amount remained substantially unchanged: most of them, though slightly lower than in 2016 (-1.4 percentage points), involve suspicious transactions for sums between €50,000 and €500,000. The biggest increase, of over 3 percentage points, was in the lowest class (sums lower than €50,000), while there were negative changes in the two classes below the highest one (see Figure 2.5).

Figure 2.5

Distribution of STRs received by amount

(in euros)



Types of transactions reported

With regard to the type of transactions reported,[55] domestic credit transfers were prevalent in 2017 too, followed by money transfers and cash transactions, categories which account overall for over 70 per cent of the distribution. There were increases in the first two types of transaction compared with the previous year, of 2 and 7.8 percentage points respectively. The significant increase in the relative weight of transfers is a result of the full entry into force since August 2016[56] of the new reporting mechanism for the operators in this category, which makes it easier to communicate a large number of transactions within the reports.

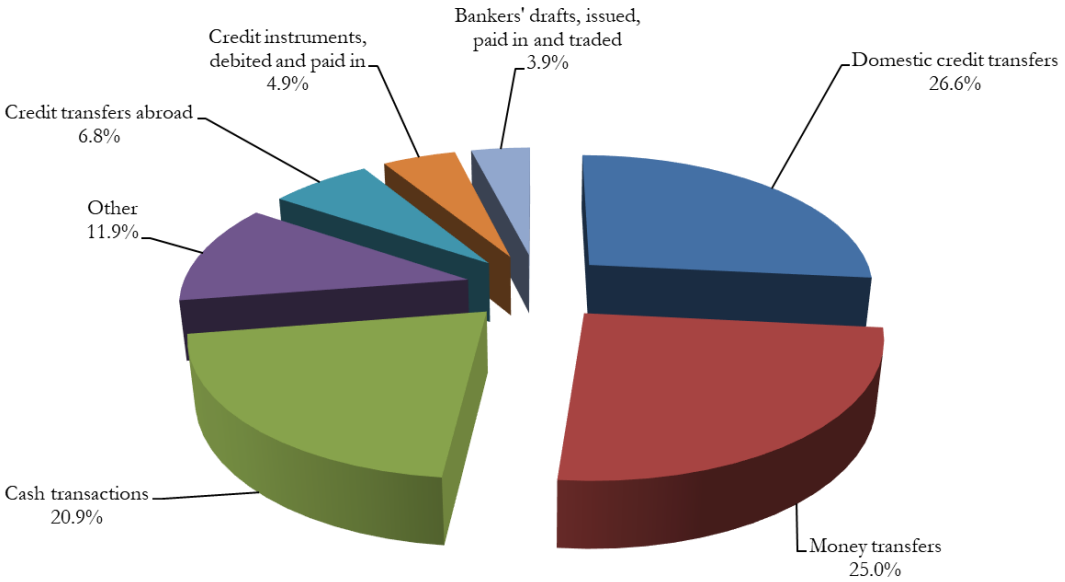
The types of transaction affected by a negative change include credit transfers abroad (-3.8 percentage points), which are often connected with the repatriation of funds following the activation of voluntary disclosure (see Figure 2.6).

[55] Percentages are calculated with reference to the number of individual transactions, not to the number of reports. It should be remembered that a single report may contain more than one transaction.
[56] See Annual Report of the UIF on activities carried out in 2016, Section 2.3.

Figure 2.6

Main types of transaction reported in 2017

(per cent of total transactions reported)



Transmission times for STRs

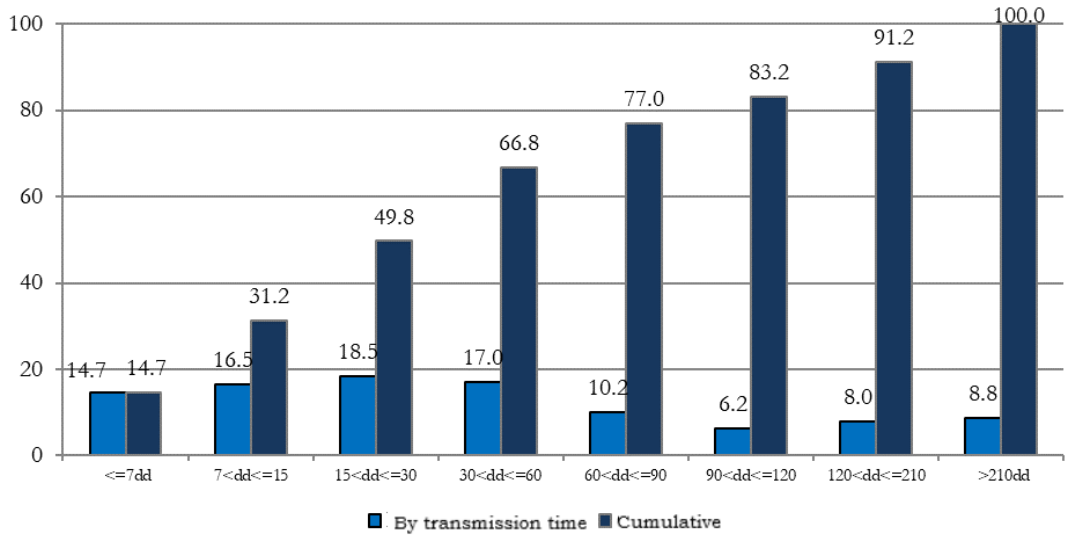
As regards transmission times, in 2017 some 50 per cent of reports were sent within one month of the transaction, 66 per cent within two months and 77 per cent within three months (see Figure 2.7). There was an increase in each of the transmission time groups compared with 2016, confirming the increased awareness of the need to reduce reporting times, especially on the part of operators who were less careful about this particular aspect in the past.

In the 15 days following the transaction, banks sent 30 per cent of their reports. The average transmission times instead remained slower for intermediaries and financial operators other than banks, as well as for gaming service providers; they sent 17 and 19 per cent respectively of their reports in the 15 days following the transaction. Transmission times were faster in 2017 too for reports relating to cash transactions (over 72 per cent within 60 days) or rather for those sent in connection with suspicious elements of a subjective nature (mostly attributable to investigations into reported persons). These reports are often characterized by a less thorough assessment process.

Figure 2.7

Distribution by transmission time of STRs received by the UIF in 2017

(per cent of total transactions reported)



Generally speaking, the difference in transmission times between the various categories may depend on the different internal analysis processes for ascertaining the grounds for suspicion, influenced by the organization and the type of activity of the reporting entity.

2.3. The quality of active cooperation

The UIF's awareness-raising initiatives

The figures for the flow of reports, though reflecting the growing awareness of reporting entities with regard to combating money laundering and the financing of terrorism, provide no indications as to the effectiveness and efficiency of their cooperation, as an expression of the ability of obliged entities to identify suspicious transactions and make prompt, complete and high-quality reports to the UIF. The vital importance of these aspects led the Unit to launch, from 2012 onwards, a series of meetings with the main reporting entities to discuss common irregularities and inefficiencies in reporting. Starting from 2014, with reference to banks, monitoring has been carried out by means of methodically observing specific indicators, the results of which are shared with the main representatives of the category in question.

In 2017 a new series of interventions was planned, consisting of meetings, formal communications and monitoring, according to a modular selection based on specific characteristics emerging from qualitative assessments made by UIF analysts and from the observation of the trends in some specifically developed indicators.

These initiatives involved 19 intermediaries, collectively responsible for 36 per cent of the reports received over the year. Of these, 13 belong to the 'Banks' category, five are payment institutions (including four money transfer operators) and one is a gaming service provider.

The main critical aspects examined in the meetings, underlined in the formal communications or analysed during the monitoring, refer both to the diagnostic ability

of reporting entities, especially in focusing on grounds for suspicion, and to the complete and correct compilation of STRs. Important meetings were held following organizational changes that involved the functions tasked with identifying suspicious transactions, because of the possible repercussions on the quality of active cooperation.

Feedback reports

As in the previous three-year period, the UIF continued to provide the main operators from the 'Banks' category with feedback reports that summarize its findings. Similar feedback reports have been prepared for money transfer operators,[57] with appropriate indicators that take account of the sector's characteristics.

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

1) the extent of the cooperation, measured by the number of reports submitted by the reporting entity in the relevant time period as a percentage of the total number of reports sent by the reference group. This provides a parameter for the entity to assess the quantity of the reports they provide;

2) timeliness, shown by the percentage distribution of reports by time period and by median transmission time. This allows the reporting entity to assess their own speed of reaction to emergent suspicious elements;

3) the ability to detect transactions that pose an effective money laundering risk, measured by indicators that capture both the risk level of the reports according to the UIF's prior financial analysis and the existence of any law enforcement investigations under way;

4) the ability to describe suspicious activities adequately and effectively in terms of the number of levels in the transactions and of the persons indicated in the report.

As has happened in previous years, the main reporting entities from the 'Banks' category have been individually assessed according to the quality and complexity of the reports submitted compared with the average levels of their category. Two indices are used that summarize the importance of the reports sent in terms of the high level of risk measured by the UIF and the investigative bodies (the composite quality indicator) and of how well the cases were described (the composite complexity indicator).

Figure 2.8 shows the positioning of the reporting entities in each of the four categories relating to the quality/complexity of their active cooperation. The scatter graph was plotted with reference to 62 operators from the 'Banks' category that submitted more than 100 reports in 2017.

The changes that affected the organization and ownership of some large banks in 2017 impacted the composition of the sample to be investigated, down by 15 units compared with 2016. Overall, the operators analysed accounted for 89 per cent of the

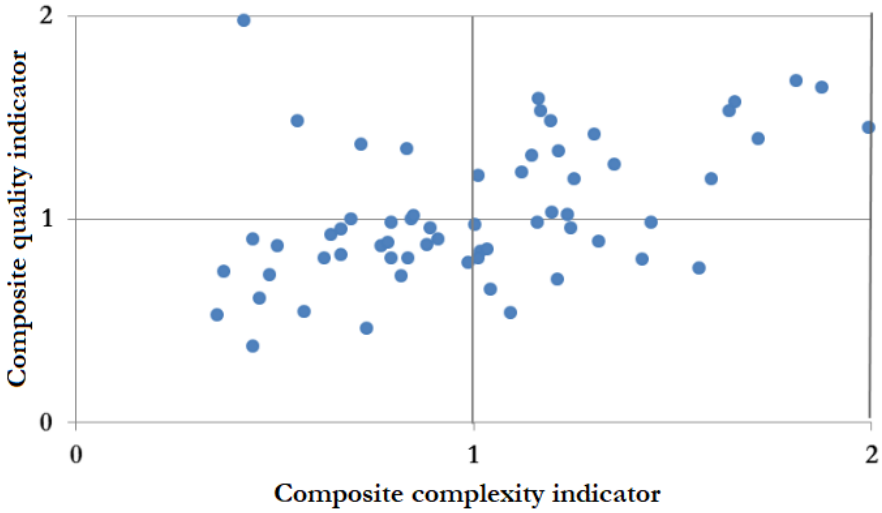
[57] These reports, currently in the trial stage, were shared with some of the operators involved in the above-mentioned meetings held in 2017.

reports received during the year from the reference category, a figure substantially in line with that of the previous year.

Compared with 2016, the number - for the sample analysed - of intermediaries submitting reports of above-average quality decreased to 40.3 per cent.

Figure 2.8

Scatter graph based on the quality/complexity indices of the reporting entities in the 'Banks' category that submitted more than 100 reports in 2017



Among the entities monitored, 19 of them, or 30.6 per cent, submitted reports of a quality and complexity higher than the benchmark. The reports of 6 entities, or 9.7 per cent, were less complex but of above-average quality, while 12, or 21 per cent of the total, sent reports with a high level of complexity but of below-average quality. Finally, 24 reporting entities, or 38.7 per cent, sent reports that were below average in terms of quality and complexity.

Precautionary reports

With regard to the flow of reports, it was found that operators belonging to various categories tended to send reports to the UIF solely motivated by requests for information from the investigative bodies in relation to clients or for notifications of seizure orders imposed by the judicial authorities. While we understand the importance of such information in raising the risk profile of the clients concerned, which leads to a careful reconsideration of their activities for potentially making a report, it should, however, be pointed out that reports of this kind are only for precautionary purposes and are of no added value for opening new fronts for the Unit's intelligence activities. In such cases, it would be advisable for obliged entities to adopt a more critical and considered approach, so that the reports sent contain not only news of investigations under way or of capital measures borne by customers, but also any other anomalies. Examining the position of a suspect may uncover personal or business relationships with other subjects (persons authorized to manage accounts, joint account holders, or counterparties for transfers of funds) which could lead to significant developments for network analysis, or further anomalies that could broaden the scope of investigation.

Assistance for reporting entities

The Unit continued to provide support in 2017 for obliged entities in registering and in sending STRs by using a dedicated email address. In 2017, the UIF processed over 2,000 requests for assistance.

2.4. Communication of cases where due diligence is not possible

In early 2017, the UIF continued to receive communications on transactions made by intermediaries to return funds for sums greater than €5,000 when they were unable to carry out adequate due diligence on their customers.

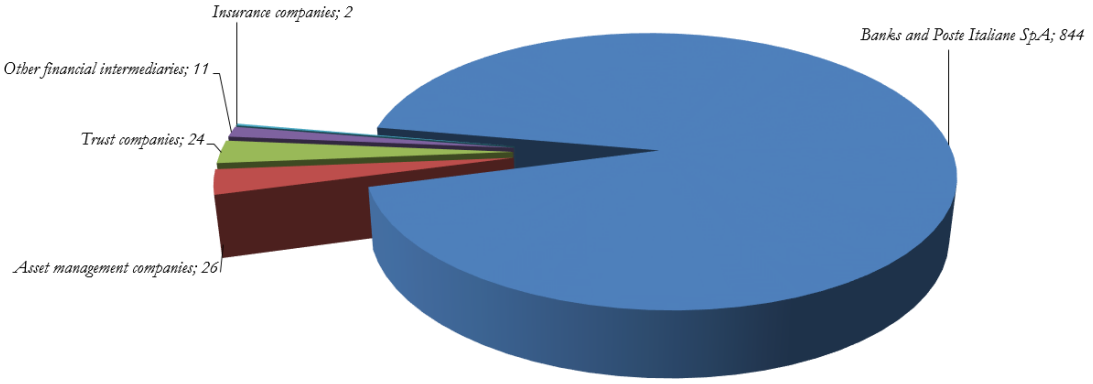
The new law (which came into effect on 4 July 2017), in regulating the obligation to abstain, no longer envisages the above-mentioned compliance, which means that this flow of information has been interrupted.

Data on returned funds

The UIF received 907 communications of this kind when the previous rules were in force, 93 per cent of which were sent by banks (see Figure 2.9). For the whole of 2016 there had been 385 from the same category of reporting entity, albeit to a lesser extent (87 per cent). As far as the sums involved are concerned, the transactions communicated in 2017 amount to about €32 million, compared with €33 million the previous year.

Figure 2.9

Communications by type of reporting entity (up until 4 July 2017)



The reporting category 'Trust companies' includes those registered on the register provided for by Article 106 of the TUB, while the trust companies pursuant to Law 1966/1939 are in the 'Other financial intermediaries' category, in line with the classification of Legislative Decree 231/2007.

Some 97 per cent of returned funds, for a total of about €31 million, were transferred to accounts held at banks with headquarters in Italy. The remaining 3 per cent involved banks with their headquarters abroad, mainly in European countries. In 24 cases of returned funds operations, STRs were submitted.

3. OPERATIONAL ANALYSIS

The UIF performs a financial analysis of the suspicious transaction reports (STRs) submitted by obliged entities and forwards them to the Special Foreign Exchange Unit of the Finance Police and to the Anti-Mafia Investigation Department, along with a technical report containing the results of the analysis.

The financial analysis conducted by the UIF comprises a series of activities aimed at redefining and expanding the context of the original report, identifying persons and objective connections, reconstructing the financial flows underlying the operations and identifying transactions and situations linked to money laundering or the financing of terrorism, thereby increasing the set of information for each report. It is a process of transformation in which the data obtained from the suspicious transaction reports are processed through automated systems, supplemented by the analysts' findings, then classified according to risk and transaction type in order to identify the most significant of them and, lastly, this information is shared in the most effective way possible so as to facilitate subsequent investigations. The process takes a risk-based approach as defined by the international standards and allows the work of the Unit to be adapted, taking into account the risks and vulnerabilities identified in the course of risk assessments and in the results of strategic analyses.

The analysis of suspicious transaction reports is central to the Unit's financial intelligence activities and is instrumental in identifying the investigative elements to be forwarded to the authorities responsible for investigating cases of money laundering, predicate offences and the financing of terrorism.

The UIF is constantly working to improve its assessment processes and add to its data sources, strengthening the selectivity and effectiveness of its institutional activities and the sharing of its results with investigative bodies.

The wealth of knowledge that comes from the selection and analysis of STRs also allows the UIF to classify suspicious transactions and to identify and define types and patterns of abnormal behaviour to be shared with the obliged entities.[58]

3.1. The numbers

In 2017 the Unit analysed and transmitted 94,018 STRs to investigative bodies (Table 3.1 and Figure 3.1). The decrease compared with 2016 reflects a similar one in incoming reports, which is attributable, as observed earlier, to the decline in reports connected with voluntary disclosure (see Table 3.1 and Figure 3.1).

[58] See Chapter 4.

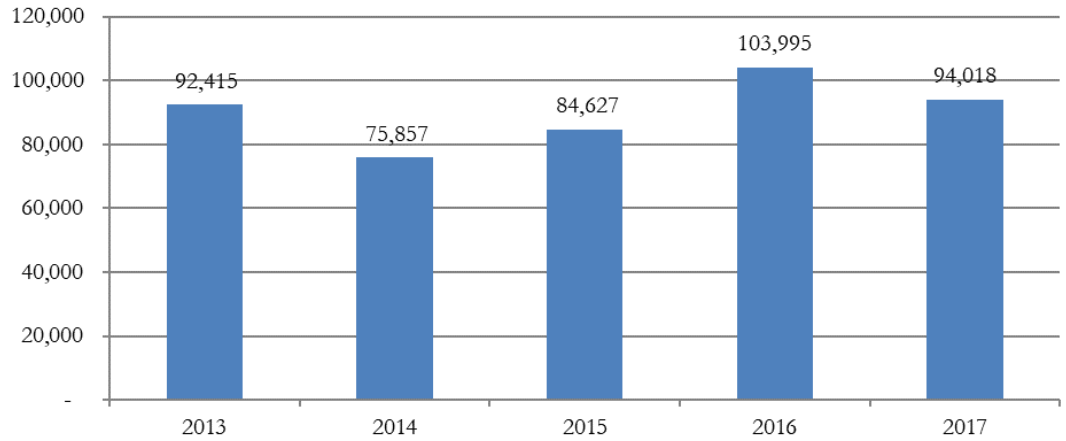
Table 3.1

Reports analysed by the UIF

	2013	2014	2015	2016	2017
Number of reports	92,415	75,857	84,627	103,995	94,018
Percentage change on previous year	*53.8*	*-17.9*	*11.6*	*22.9*	*-9.6*

Figure 3.1

Reports analysed by the UIF
(absolute values)

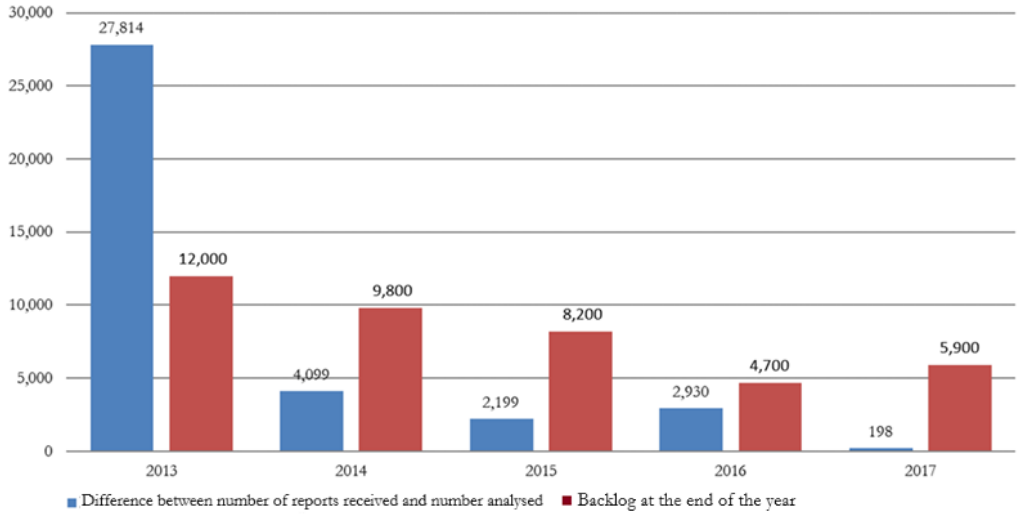


In 2016, the reports connected with voluntary disclosure accounted for over one fifth of the total STRs received by the Unit. These reports, characterized by recurring elements and often sent for precautionary purposes, were channelled into an analysis aimed at ensuring a standard and rapid processing, once it had been established that there was nothing requiring in depth analysis. Reports of this kind decreased considerably in 2017, accounting for only 6.5 per cent of the total. The different contexts of voluntary disclosure, given their variety, require more complex processing, in line with the complexity of individual cases; the need for a detailed weighting of the risk elements underlying the transaction reported requires adequate time for processing.

The UIF continues to deal effectively with the STRs received: the progressive improvement of work processes and methods allowed further inroads to be made into the backlog of reports, standing as of 31 December 2017 at around 4,500 reports, against 4,700 in 2016; there was a positive balance of 198 between the reports analysed and those received during the year (see Figure 3.2).

Figure 3.2

Efficiency of STR work processes
(absolute values)



3.2. The analysis process

In accordance with international standards, the financial analysis process is divided into a series of activities designed to identify which suspicious transaction reports are considered to be well-founded and warranting further investigation, to assess the actual degree of risk involved and to decide how they should be handled by drawing upon a variety of information sources.

The collection and the management of the STRs are supported by a computer system (RADAR) which receives the reports and is the first point of data entry. The recurrence of suspicious behaviour (even by different operators) or cross-checks with other transactions produce an initial frame of reference for the anomaly that elicited the report.

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

In the ten years since it was founded, the UIF has been consistently developing its methods and instruments in order to deal with the constant increase in the level of active cooperation provided by reporting entities. The increase in staff, which has been moderate but sustained, its professional qualification and the development of increasingly sophisticated technical tools have allowed the Unit to carry out its tasks by adopting a risk-based approach suited to the resources available, meeting the new challenges posed by a rapidly and ever-changing scenario one by one, and consolidating its position as Italy's financial intelligence unit over time.

Thanks to the experience it has acquired, the UIF has gradually been able to transform the procedures adopted, by expanding the analyses carried out beyond the scope of the individual transactions reported. The constant growth in reports received has brought such a large critical mass of cases of potential money laundering and financing of terrorism (over 600,000 reports between 2008 and 2017) to the Unit's attention that it has progressively achieved a greater amount of observed phenomena. Micro analysis, which aims to reconstruct financial flows and any classification of illegal behaviour underlying the facts reported (to make subsequent investigations easier), has been coupled with a more wide-ranging approach, aimed at identifying the same recurring features among the cases examined.

Modelling

The long-term observation of such recurrences has allowed us to define types of anomalous behaviour which, thanks to the findings of the analyses, have been correlated where possible with the criminal activities which have produced the observed financial patterns. Thanks to this approach, some simplified analytical processes have been developed over the years that, when the above-mentioned elements recur, enable reports to be swiftly connected to a specific phenomenon, and types, patterns and indicators have been defined, in order to make the detection of suspicious transactions easier for obliged entities.

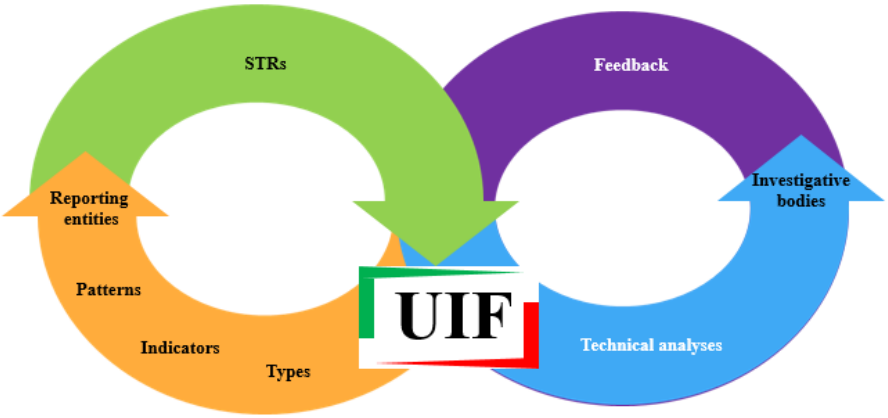
On the one hand, this information circuit creates some advantages by speeding up the various phases of the analysis and strengthening its conclusions, and on the other hand helps the reporting entities when fulfilling their active cooperation obligations, since they can exploit the support provided by the communications and the abnormal behaviour patterns developed by the Unit following its analyses.

The active cooperation cycle

Thanks to the synergies developed between the various players in the system, a mechanism has been created whereby the information entered into the active cooperation circuit in the form of STRs returns to the reporting entities, following a complex process which exploits their most important aspects and turns them into a model.

Figure 3.3

The active cooperation cycle



It is not only for the most common recurring situations that the search for typical elements has produced significant results. The same approach, applied to reports with

new elements that cannot be attributed to well-known typologies and that may be symptomatic of new criminal trends, has enabled the Unit to focus on areas of emerging risk, not yet fully explored by reporting entities. It has happened that analysing individual transactions which did not appear to be particularly risky actually brought some very important events to light, which then prompted further autonomous analyses to verify whether the same pattern might be found in similar cases.

Threshold-based communications

Further important changes await the UIF in the near future: the implementation of new measures concerning threshold-based communications will have a significant impact on the field of active cooperation too. These communications will focus on transactions not characterized by actual elements of suspicion, but identified exclusively on the basis of objective criteria which make them particularly interesting with a view to combating money laundering and the financing of terrorism.[59] As well as expanding the Unit's outlook by making another database available from which to draw useful elements for STR analysis, the availability of this information set will make it possible to set up autonomous pathways for analysing and monitoring potentially anomalous flows.

3.3. Risk assessment

A proper risk assessment in the various phases of the STR appraisal process is important for the financial analysis and in the subsequent investigative phases. The assessments summarize a number of factors.

The most important factor is the risk of money laundering or the financing of terrorism attributed to the transaction reported by the obliged entities, which is expressed on a 5-point scale.

The level of risk assigned by the reporting entity helps to determine the automatic rating attributed by the RADAR system to each STR.

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

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

The UIF is constantly working on improving its tools and methodologies (including econometric techniques) so as to provide guidance which, together with the rating mechanism detailed above, makes the processing of reports more efficient.

[59] See Section 1.3.1.

Careful risk weighting is a key principle of the entire system for preventing money laundering and the financing of terrorism and is also a central part of the process for analysing suspicious transaction reports. The risk assessment associated with each report influences how it is dealt with and analysed. At the same time, the risk assessment is significantly influenced by this process, given that the details that emerge from in-depth financial analysis might downgrade or raise the risk level automatically attributed to the reports when they enter the system.

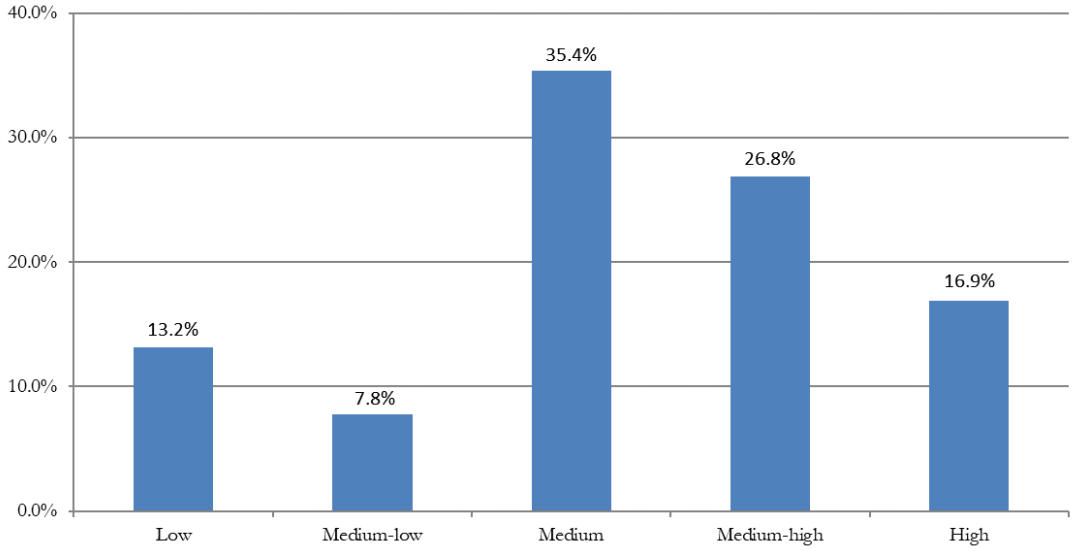
The UIF's final rating

In 2017, at the end of the acquisition and analysis process, 44 per cent of the STRs analysed by the Unit were considered to be high risk (high and medium-high ratings), 35 per cent medium risk and 21 per cent low risk (low and medium-low ratings; see Figure 3.4*)*. A comparison with the data for 2016 shows a fall of about 9 percentage points in the reports classified as medium-risk, offset by an increase in the reports considered to be low and medium-low risk. This trend was mainly due to the more selective approach adopted by the analysts, which has led to a more limited use of the medium rating for the benefit of subsequent investigations.

Figure 3.4

Reports analysed in 2016: distribution by final rating

(per cent)



In 2017 there was an increase in the rate of convergence between the results of the assessments made by the reporting entities, summarized by the risk level they assigned to the reports, and those represented by the rating assigned by the UIF at the end of the analysis process. The reports that basically received the same rating accounted for 44 per cent of the total, against 42 per cent in 2016. This convergence was also more significant in 2017 for reports considered to be less important (see Table 3.3).

Table 3.3

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

		Risk indicated by the reporting entity			
		Low and medium-low	**Medium**	**Medium-high and high**	**Total**
UIF Rating	**Low and medium-low**	14.9	5.1	0.9	**20.9**
	Medium	17.8	11.7	5.8	**35.3**
	Medium-high and high	10.1	15.9	17.6	**43.6**
	Total	**42.8**	**32.7**	**24.3**	**100.0**

Note: the cells in light blue give the percentages of reports for which the risk class indicated by the reporting entity and the final rating assigned by the UIF correspond.

3.4. The methodology

The processing of STRs starts with a 'first-level' analysis, which applies to all reports received, in order to evaluate the actual level of risk and decide on the most appropriate type of processing.

On the basis of the information acquired automatically or from other sources, the grounds for suspicion of money laundering and the need for further action are evaluated.

If some of the preconditions are present (full description of the activity and the grounds for suspicion; suspicion based on a well-known typology; impossibility of proceeding with further investigations; and the chance of sharing the information rapidly with the investigative bodies), the STR can be accompanied by a simplified report, thus optimizing processing times.

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

At this stage, there are many investigative options and tools available. It is possible to: contact the reporting or other obliged entities to obtain further information; consult the national database of financial account holders to identify the banks with which the suspects hold their accounts; access the national tax database; and involve foreign FIUs if the transaction has cross-border implications or if significant repetitions emerge from FIU.NET's periodic multilateral matching software ('Ma3tch').

Financial analysis is therefore a complex process, divided into various components, whose sequence cannot usually be predicted upstream. The variety of contexts described in STRs, reflected by the broad range of reporting agents and of

situations considered important by the legislature means that a 'tailor-made' approach is required that can adapt to the particular features of each individual case. The initial and delicate phase of the process, namely the first-level analysis, is in fact guided by this approach.

First level analysis

In this phase the information sent by the reporting entities is automatically combined with what is already available to the UIF, thanks to the functions provided by the data warehouse[60] which has gradually integrated most of the data base used by the Unit. The picture that emerges, which already includes the risk level automatically assigned by the system, is then brought to the attention of an analyst who decides on the most suitable investigation pathway. To this end, it is vital for the reporting entities to present the facts correctly to the Unit; the appropriate filing of the information most relevant to the event reported may be crucial for a more rapid interception of the highest risk cases. In the same way, the ability of the analysts to promptly recognize and make full use of the inherent potential of every report is fundamental during this phase. The Unit is constantly working on perfecting technical instruments that can assist analysts in their delicate work. With reference to situations most at risk, several indicators have been identified over time, relating to the subjective profiles of natural and legal persons, to any economic and personal relations detected between them, to sectors of activity, and to the geographic areas in which funds are located or have their source or allocation. Their recurrence and combination, thanks to automatic extractions, may contribute to showing the potential risk underlying the reported events and indicating a suitable way to process them.

Access to investigative information

The picture is completed by the indicators of investigative interest received from the Finance Police which, by providing summarized information about individual STRs that could be of interest in the light of any previous offences committed by reported subjects, can significantly influence the choice of analysis. The content and methods of this flow of information, governed by an agreement stipulated in 2014 between the UIF and the Finance Police to remedy the lack of access for the Unit to the investigation files, will soon be reconsidered in light of the reform of Legislative Decree 231/2007. The new Article 12(4) will fill this gap by establishing that the investigative authorities shall supply the investigative information necessary to enable the UIF to carry out its analyses, with the details to be agreed upon.

Second level analysis

The reports which, given the outcome of the first-level analysis, do not require any further investigation and are sufficiently thorough and complete to make it easy to connect any anomalies to well-known financial phenomena, are channelled towards faster processing streams. At the end of this phase any reports that do require further investigation are submitted for second-level analysis. To this end, reports are assigned to an analyst, also in light of any particular issues or areas of expertise acquired in processing previous reports traceable to similar events.

Second-level analysis involves a broad spectrum of activity which has expanded over time together with the most significant developments in the sector's legislation.

[60] The data warehouse integrates most of the information available to the UIF and makes it possible to access the relevant information more rapidly for the investigation of suspicious transactions, by exploring the data both in summary form and in the greatest level of detail. See Annual Report of the UIF on activities carried out in 2015, Section 4.4.

The gradual implementation over the years of measures that increasingly focus on the need for obliged entities to have a high level of knowledge about their customers and of their transactions has had a positive impact on active collaboration as well. The move towards acquiring more detailed information about the nature and scope of customers' transactions, which also includes requests for documentation to support declarations provided by customers', in accordance with the established measures for adequate due diligence on the part of obliged entities, has opened up new horizons for financial analysis. Cases in which further analysis of a report ends with an examination of bank accounts and financial reports in order to reconstruct the origin and destination of the funds which were the object of the report are increasingly rare. It is far more common for a correct interpretation of the facts reported and an appropriate classification of the crimes underlying them to lead to more sophisticated assessments, focusing on an analysis of further documentation provided by reporting entities to support their suspicions or tracked down by the analysts by consulting open sources and the various databases available to the Unit. It happens more and more often that, in the context of second-level analysis, it may be necessary to consult corporate balance sheets, commercial invoices, contracts for the supply of goods or services, or for the sale of properties, credit or company shares, private contracts, commercial agreements, tax returns and any other kind of documentation that justifies the financial anomalies reported or that substantiates reasons for suspicions more fully. The greater involvement of non-financial operators, especially professionals, in active cooperation has been crucial to this process. These categories of reporting entities have a different insight into their customers' operations compared with that of financial intermediaries and are able to find anomalies that are often complementary to those inherent in the movement of funds.

SAFE

Finally, the results of information exchanges with the corresponding foreign authorities make a significant contribution to expanding the outlook for analysts.[61] There were some important innovations on this front in 2017: the project that established the inclusion of communications regarding international cooperation in the RADAR system was completed, thereby guaranteeing the automation of the phases for transmitting and receiving the requests and providing for the integrated management of the results. In light of the results of the Mapping Exercise carried out last year by the FIUs' Platform, the first experiment in joint analysis between various European FIUs was also launched, coordinated by the UIF. In order to improve the quality of international cooperation by overcoming the obstacles created by the many differences between the institutional and operative aspects of the FIUs, a bottom-up approach was adopted. It started with the parallel analysis of a case of international money laundering conducted by the FIUs of all the countries involved, which should lead to the development of coherent and effective joint methods and practices. This analysis, which is still being developed, has involved four FIUs so far and is based on the sharing - in real time and on a multilateral scale - of all the information gathered by each Unit as part of its intelligence activities.

Joint analysis

[61] See Section 9.1.

Starting from June 2017 and in line with a specific regulatory measure,[62] the Unit has begun to receive cross-border suspicious transaction reports (XBD, or cross-border dissemination) identified by EU FIUs applying shared criteria of selection and importance. These reports, which are automatically exchanged via the FIU.NET channel, are helping to expand the UIF's wealth of knowledge by finding important subjective and objective links and tracing financial flows even beyond national borders, as well as by selecting cases worthy of further analysis more effectively. From a proactive point of view, they can also orient the combating of money laundering and financing of terrorism towards a preventive strategy, so as to identify criminal behaviour that is not intercepted by the national network of the obliged entities.

Cross-border reports

3.5. Issues of major concern

Operational analysis has revealed specific issues that have been the subject of further investigation.

3.5.1. Anomalous investments by social security institutions

The UIF's investigations have brought to light some investments by social security institutions that appeared to have anomalies concerning the sale prices of properties or how their assets were managed. In past years, one particularly significant case concerned an EU investment firm, traceable to an Italian group, which had taken over the management of almost all the assets of the social security institution in question. Criminal proceedings arose from investigations by the judicial authorities, also in relation to cases of corruption, and the Court of Auditors ordered the president of the institution to pay a significant amount of compensation for the damage suffered by the same institution.

The potentially high riskiness of property and financial investments made by social security institutions was also confirmed by the results of the analyses carried out in 2017, which highlighted the anomalous operations of various subjects in some institutions of this kind.

Further analysis underlines the central role that advisors may play in managing the financial assets of such institutions. They act as consultants and give support that is often instrumental in drawing up investment policies, although these are technically entrusted to the institution's decision-making body, because its members are usually elected from their professional sector and therefore do not necessarily have specific financial expertise.

Significant anomalies emerged in reference to investment in movable and immovable assets in which various Italian and foreign companies also participated, in some cases traceable to the same centres of interest. There were substantial economic returns, direct and indirect, for these companies, sometimes refunded, in part, to those

[62] Article 53 of the Fourth Directive envisages that 'when an FIU receives a report to point (a) of the first subparagraph of Article 33(1) which concerns another Member State, it shall promptly forward it to the FIU of that Member State'.

managing the said social security institutions as invoiced payments for consultants. The involvement of EU management companies traceable to Italian citizens and operating in Italy under the principle of mutual recognition is a recurring feature in the transactions described.

Generally speaking, the analyses carried out showed how the investment choices of some social security institutions can sometimes be influenced by potential conflicts of interest between institution officials and external firms authorized to manage their assets or to provide consultant services. This was possible because of the incomplete legislative framework regulating this matter. Legislative Decree 98/2011, in tasking Covip (Italy's supervisory authority for pension funds) with supervising the institutions in question, announced the imminent adoption of measures regarding the investment of financial resources, conflicts of interest and depositary banks, but they have never actually been implemented.

3.5.2. The sale of non-existent VAT credits

Further analysis of various STRs, mostly sent by professionals, led to a focus on possible abuses in the selling of VAT credits. Such contracts allow the ceding firms to free up the credits receivable from the financial administration and come into possession of liquidity in less time than it would take for their rights to be recognized.

The institution is regulated by sectoral rules, according to which VAT credit can only be sold if it comes out of the annual tax declaration and repayment has been requested in advance.

Once these prerequisites have been met, the sale must take place by means of a public act or a private authorized contract, and further requirements for disclosure to the financial administration must be complied with which, among other things, aim to prevent fraudulent conduct.

The analyses carried out by the Unit have shown how the VAT credits sold are often fictitious, as they have been generated by recording invoices for non-existent operations. This fraudulent mechanism works due to the involvement of 'shell' companies (with no real organizational structure and managed by straw men or nominees) that sell non-existent goods or services for significant sums and issue invoices in the name of the purchasing firms; the latter in turn carry out fictitious export sales operations of the goods purchased, without paying any taxes, to various foreign firms traceable to the same subjects, thereby generating a large amount of non-existent VAT credit.

This operation allows the transferee companies to reduce their tax burden, through wrongful VAT credit compensation with existing tax debts; on the other hand, the transferor companies can acquire the liquidity deriving from the monetization of the false transferred credit.

The fictitious VAT credit is sometimes used to provide capital to newly created companies, partly to satisfy the economic and financial requirements needed to take part in important public procurement projects, which are sometimes linked with corruption. Professionals have also been found to be part of this fraud, in their role as certifiers of VAT credits.

Further analyses have, on the one hand tried to reconstruct the subjective profile of the transferor and transferee companies and their financial operations, including abroad, and on the other hand to identify the bills of sale and the means of payment for the amount agreed. The analyses have revealed sales of non-existent VAT credits, mostly concluded in the central and northern regions for very large sums, the revenues for which have been converted into cash or used to make bank transfers, including abroad, to 'connected' persons or for signing investment contracts.

From a subjective point of view, the sectors of activity of the shell companies involved vary from logistics services and goods transport to products for building and for the catering sector, to wholesale trade in petroleum products and travel agencies. It often happens that, just before the sales, the companies, including cooperatives, record the arrival of new directors who are often young and foreign and appear to take on the role of nominees. In some cases, connections have been found between corporate representatives and organized crime, using both information acquired from open sources and data provided by some reporting entities, who have been asked to do so by the judicial authorities.

There have been several examples of VAT credits being sold at considerably lower prices than their nominal value, with no apparent justification; payments are usually settled in particularly advantageous ways for the purchasing firms, such as the total repayment in instalments of the amount established or deferred payments with no interest.

3.5.3. Fraud in the Tradable Certificates for Energy Savings (TCES) market

In 2017, reports were received concerning Energy Service Companies (ESCOs), active in the Tradable Certificates for Energy Savings sector or Energy Efficiency Titles, as they are known in Italy (TCES[63] or white certificates) issued by the Italian Power Exchange (Gestore dei Mercati Energetici SpA - GME[64]) to certify reductions in consumption achieved by interventions to increase energy efficiency.

These certificates are the basis of the energy incentive schemes for efficiency measures based on an obligation to save energy for, among others, distributors of electric energy and natural gas.[65] These obligations can be observed by means of 'first person' interventions, and by receiving the white certificates directly from the GME, or rather by making use of certificates assigned to another operator who, having achieved

[63] Each TCES certifies a saving, in tonnes of oil equivalent (TOE), in the consumption of electricity, methane gas or any other fuel.

[64] The GME was set up by the Energy Services Manager (Gestore dei Servizi Energetici - GSE SpA), a company wholly owned by the Ministry of Economy and Finance (MEF). The GME organizes and manages the electricity, natural gas and environmental markets.

[65] In particular, the TCES are issued by the GME to subjects, pursuant to Article 7 of the Ministerial Decree of 28 December and to Article 5 of the Ministerial Decree of 11 January 2017, based on savings achieved and communicated to the GME by the GSE, in accordance with the measures applicable. The GME also issues TCES to certify energy-saving actions in high-efficiency cogeneration plants (CAR), whose certification is carried out by the GSE, in order to implement the measures referred to in the Decree of the Minister of Economic Development of 5 September 2011.
See http://www.mercatoelettrico.org/it/mercati/tee/cosasonotee.aspx.

energy savings over and above the annual target, decides to sell them. The regulatory requirements containing the above-mentioned obligations are therefore the reason for the very existence of the TCES market, organized and managed by the GME and which end users access by means of the above-mentioned ESCOs.

The trading of TCES by the latter has been reported several times because of the massive financial flows between ESCOs and the GME. Further investigation into this category of reports has revealed clear anomalies relating to both the characteristics of ESCOs and the financial transactions carried out. Regarding the characteristics, there have been several examples of newly formed engineering consultancy firms with low capitalization levels (usually the minimum required by law) and no recourse to banking/financial credit; such firms are often found to be managed by persons with no experience in the energy sector. Despite this, the firms in question have registered a high turnover since their first financial year which, from a financial point of view has meant they received significant payment flows from the GME, presumably linked to TCES trading. In some cases, this has led to the payment of annual dividends that are 150 times the capital invested in setting up an ESCO.

Some analyses revealed the marked difference between the price paid by third parties bilaterally, i.e. off-market, and the much higher sum earned by selling the certificates on the market. There have been equally serious concerns over the way in which the money from the GME has been used. In particular, it has emerged that it has been partially transferred abroad (Romania, Bulgaria and Malta) to other consulting firms; the remainder has been used to pay dividends, for real estate investment and for money transfers relating to payments of generic invoices.

With regard to the beneficiaries of these credit transfers it emerged that, in some cases, they are subjects that have been reported because of repeated cash withdrawals or have already been investigated by the judicial authorities.

3.6. Reports requiring no further action (NFA)

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

Over the last ten years the UIF, in its role as a focal point between reporting entities and the institutions responsible for combating money laundering and the financing of terrorism, has found out that an approach based on maximum information sharing is always rewarding. However, effective intelligence action assumes that shared information is adequately filtered, classified and selected according to the risk it defines.

Legislative Decree 90/2017 intervened by modifying the form but not the substance of the previous measure. The new wording[66] no longer refers to the 'dismissal' of reports, but instead envisages that the UIF stores reports that raise no

[66] Article 40(1)(f), Legislative Decree 231/2007.

reasonable suspicions of money laundering or terrorist financing for ten years, and ensures that the investigative authorities can consult them if necessary.

In light of this measure, if no elements are detected during the analysis of a report to support the suspicions of a reporting entity, substantiated by the attribution of a prosecution bias rating that certifies that the reported entities have no previous offences, then the STR will be classified as being low-risk. In order to ensure a constant alignment of the UIF and the investigative authorities' databases, it is deemed preferable to continue sending reports of this kind, but through a separate stream.

In this way, the Unit - in compliance with the above-mentioned regulatory framework - balances the need to guarantee the full sharing of its information with the investigative authorities with an effective selection process; it can then concentrate on the cases in the total reporting flow requiring greater attention in view of the risk associated with them, and conversely to identify cases with no risk of money laundering or financing of terrorism.

In 2017, about 16,000 reports were identified which, according to the Unit's analyses, showed no evidence of any significantly suspicious elements. This is equal to 17 per cent of the total number of reports analysed in 2017, and a sharp increase compared with the figures for 2016. This trend was influenced by the decline in reports referring to voluntary disclosure transactions, which are usually channelled towards a specific process that excludes the assignment of a minimum rating, generating a result in line with the figures from previous years.

Table 3.4

Reports requiring no further action (NFAs)

	2013	**2014**	**2015**	**2016**	**2017**
Reports analysed	**92,415**	**75,857**	**84,627**	**103,995**	**94,018**
NFA reports [1]	7,494	16,263	14,668	10,899	16,042
NFA reports as a percentage of all reports	*8.1*	*21.4*	*17.3*	*10.5*	*17.1*

[1] For the years prior to 2017 refer to the archived reports.

Around 76 per cent of the NFA reports were rated as low or medium-low risk by the obliged entities, while only 3 per cent of reports were deemed of high or medium-high risk (Table 3.5).

Table 3.5

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

(percentage composition)

		Risk indicated by the reporting entity			
		Low and medium-low	**Medium**	**Medium-high and high**	**Total**
UIF Rating	**Low**	69.6%	0.7%	0.0%	**70.3%**
	Medium-low	6.5%	19.8%	3.4%	**29.7%**
	Total	**76.1%**	**20.5%**	**3.4%**	**100.0%**

The UIF returns information to reporting entities about reports that have been analysed and assessed as being risk-free. These communications are currently sent via the Infostat-UIF platform, thanks to a new and specifically designed function that favours the recipients in the acquisition of these data within their information systems with a view to further processing.[67]

3.7. Suspension orders

The UIF, on its own initiative or at the request of the Special Foreign Exchange Unit, the Anti-Mafia Investigation Department, the judicial authorities or foreign FIUs, may suspend transactions that are suspected of involving money laundering or the financing of terrorism for up to five working days, as long as this does not jeopardize the investigation.

Suspensions are usually ordered in response to unsolicited communications from banks that provide advance information on the contents of suspicious transaction reports.

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

In 2017 there was a considerable increase (about +70 per cent compared with 2016) in the flow of information sent by reporting entities as regards exercising powers of suspension:[68] 214 cases compared with 126 in 2016. In 38 cases (31 in 2016) the investigation conducted by the Unit together with the investigative authorities led to a transaction suspension order, with an overall value for suspended transactions of €66.4 million, against €18.9 million in 2016. The average value of suspended transactions increased to €1.7 million in 2017 from €609,000 in 2016. The rules do not envisage the UIF receiving feedback as to whether the competent judicial authorities have

[67] See Statement by the UIF of 24 May 2018.
[68] Article 6(4)(c), Legislative Decree 231/2007.

subsequently seized funds, but it was informed by reporting entities that this measure was taken in at least 71 per cent of cases.

Table 3.6

Suspensions					
	2013	**2014**	**2015**	**2016**	**2017**
Number of transactions	64	41	29	31	38
Total value of transactions *(millions of euros)*	61.9	45.5	16.7	18.9	66.4

With regard to the type of reporting entity, in 2017 the most evident category was once again insurance companies, with 168 investigations for suspension purposes (about 79 per cent of the total), against 57 in 2016 (about 46 per cent of the total). The contribution made by banks continues to decrease, with 18 per cent of investigations compared with 33 per cent the previous year, though banks are still the category with the highest number of STRs. In line with these figures for reporting entities, the information received in 2017 dealt mainly with insurance policy transactions (especially early redemption or upon expiry), which accounted for about 79 per cent of the total. A smaller share of cases involved cash withdrawals, requests for banker's drafts and credit transfers in Italy or abroad.

Among the important innovations introduced by Legislative Decree 90/2017, the possibility of suspending suspicious transactions at the request of foreign FIUs is worth mentioning. These are cases requiring the adoption of operational procedures in close coordination with foreign counterparties whose regulations may differ significantly from those in Italy.

3.8. Information flows and investigative interest

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

The STR processing cycle ends with the Anti-Mafia Investigation Department and the Special Foreign Exchange Unit receiving feedback on the results of investigative analyses carried out on situations brought to their attention.

While the information in the indicators of investigative interest that is acquired during the initial phase of the analysis refers to any previous offences committed by reported entities and may significantly influence how the report is processed, the feedback on the investigation results arrives after the UIF's work has been completed, but it is still a valuable tool for the functioning of the system.

This information provides the Unit with a definitive picture of the importance that the anomalous cases intercepted by reporting entities and enriched by the valued added by financial analysis have acquired, once the intelligence process has been completed.

The information flow thereby becomes an important litmus test for the UIF, in order to assess the effectiveness of the analytical methods used and the selection choices made, also with a view to guiding future activities.

In 2017, the assessments made by the Unit of the actual risk level in the cases examined were consistent with the results of the analyses carried out by the Special Foreign Exchange Unit of the Finance Police. For almost all of the reports (99.3 per cent) given a low final rating by the Unit, this was followed by an indication of no interest in investigation from the authorities.

A growing rate of convergence in the assessments was also found when examining the feedback information provided by the Anti-Mafia Investigation Department: some 98.7 per cent of the reports analysed were sent with the three highest risk ratings, 57 per cent with the highest level.

The information flow in question has been improved and enriched over time. Lastly, the UIF now also receives feedback about reports which, based on the results of the pre-investigation analyses, are judged to be of interest due to possible administrative violations.

4. PROFILE CHARACTERISTICS AND TYPOLOGIES

The UIF's operational analysis of suspicious transaction reports makes it possible to identify 'profile characteristics' that are constantly monitored and updated. These are recurring elements that are important for assessing the threat posed by money laundering and the financing of terrorism, such as the improper use of certain financial instruments and payment methods, the geographical location of transactions, the economic sectors at greatest risk, the precise subjective profiles of the persons and entities reported and the complex and opaque company structures designed to disguise beneficial ownership.

Using these profile characteristics, it is possible to identify the 'typologies' that define at-risk operational patterns and behaviour profiles. The UIF uses the typologies to classify STRs and to provide updated information to obliged entities in order to help them detect suspicious transactions. In a spirit of active collaboration, the UIF publishes its results as 'Casistiche di money laundering' in the series Quaderni dell'Anti-money laundering.[69]

In 2017, the UIF's financial intelligence activity continued along several parallel lines. Well-established methods were used again, including the analysis of reports relating to well-known schemes and typologies, which have been tested extensively over the years and are now easily detected by reporting entities, though representing no less of a risk for the integrity of the economic and financial system. On the other hand, some analyses brought to light less well-known phenomena involving the anomalous use of new channels, financial instruments and legal instruments. These new methods are less easily recognized by obliged entities and therefore they are not reported as often; however, they may represent new trends in money laundering or the financing of terrorism. If the reporting entities can identify them promptly and the UIF can recognize their potential and trace their ramifications, it will be possible to ensure that preventive action can keep pace even with the constant developments in criminal methods.

Several intelligence projects on major topics launched in the previous two years began to produce results,[70] giving rise to highly complex investigations that eventually led to on-site and off-site inspections. The findings, which were notified to the investigative bodies, came to the attention of the competent judicial authorities, spawning new lines of inquiry or contributing important material for ongoing investigations. These outcomes not only confirmed the value of conducting in-depth analysis, but also prompted the Unit to process the information using a recently developed system designed to highlight typical features of the illegal practices and provide the reporting entities with more detailed feedback. Currently, the Unit is fine-tuning patterns of anomalous conduct relating to these new practices.

[69] See also Section 10.5.

[70] See the UIF's Annual Report for 2016, Section 3.5.

4.1. Profile characteristics

Cash

In line with the findings of pan-European research,[71] which places Italy at the top of the list of countries for cash use, a large number of reported transactions concerned this type of activity.[72] Cash, which is characterized by an extreme ease of use and a lack of traceability, is useful for a wide range of illegal purposes. Overall, the percentage of reports that were found, after analysis, to relate to the anomalous use of cash was slightly up on the previous year (33 per cent, against 31 per cent in 2016). The rating assigned by the Unit's analysts confirms, however, that most of the reports related to low-risk transactions: more than 60 per cent of low-risk and medium-risk STRs concerned the use of cash. It is to be hoped, therefore, that when the system of threshold-based communications comes into effect, it will have an impact on the related reports, limiting them to cases in which, alongside the elements of risk associated with the nature of the instrument there are additional anomalies relating to the objective or subjective context, thus giving rise to a suspicion of money laundering or terrorism financing. In all other cases the information on cash movements above a given threshold will be collected in the Unit's database for potential use for intelligence purposes, but in the form of threshold-based communications.[73]

Cyber fraud

Various reports received during the year referred to transactions relating to cyber-crime, not only against consumers but also against businesses and even financial intermediaries. In addition to crimes such as phishing, already widely reported by obliged entities, there are now more sophisticated illegal practices directed against, for instance, insurance companies. Some reports have alerted the UIF about payments of claims credited to accounts or prepaid cards in a different name to that of the legitimate beneficiary listed in the transfer documentation. In-depth analysis has revealed that by hacking into the insurance companies' IT systems, the criminals have replaced the client bank details associated with the policies with new details of accounts in the names of other persons who immediately withdrew the sums credited or transferred them abroad.

Fraudulent use of SDDs

In other instances, fraudulent use of Sepa Direct Debits (SDDs), i.e. pre-authorized encashments, was reported. With SDDs, the creditor's bank notifies the debtor's bank that a payment order has been issued allowing the creditor to collect sums from the debtor's account. The fraudsters target idle or sleeping accounts, setting up false orders to pay, such as invoices, tax adjustments or property management charges. The sums illegally credited are used immediately, often by means of multiple transactions that are hard to trace and make it impossible to recover the money. Thanks to international cooperation it has been possible to detect similar frauds targeting foreign businesses involving non-existent investment agreements.

By tracing the route followed by the money, often with the assistance of foreign FIUs, the Unit has been able to establish links between some cyber frauds that were originally the object of separate reports. Closer analysis has revealed the repeated use of the same pre-paid cards or accounts, including foreign accounts, to move stolen funds. This is evidence that the various cases reported are probably attributable to international

[71] See H. Esselink and L. Hernandez, (2017), 'The use of cash by households in the euro area', ECB, Occasional Paper Series, 201.
[72] See Section 2.2.
[73] See Sections 1.3.1 and 3.2.

criminal organizations. In fact, several investigations in Italy and abroad have brought to light the existence of criminal organizations set up in the form of virtual networks, whose members, often of different nationalities, rarely meet in person. These organizations exploit the ease of communication, anonymity and accessibility of the IT instruments needed to perpetrate the crime and are active throughout the whole value chain, sharing out the profits among the various segments involved (software development, sale of cyber-attack tools on the dark web, management of breached computer networks, and receipt and transfer of illegal gains).

Money transfer STRs

An aggregate analysis of STRs from money transfer operators brought to light some anomalies worth looking into further, although not all of them were identified immediately. The majority of reports concerned geographical inconsistencies, i.e. the country of origin of the person making the remittance was not the same as the country of destination of the funds. Depending on the location, such cases may relate to migrant trafficking, as subsequent investigation revealed on several occasions. It emerged that while the phenomenon was found to occur in all areas of migrant arrival, reports involving remitters of African origin were located chiefly in Sicily, those where the remitters were of Middle Eastern origin were concentrated in Puglia, and Calabria saw remitters of both origins.

Migrant trafficking

The main characteristic of financial transactions connected with suspected cases of aiding and abetting illegal immigration is the highly fragmented nature of the transfers presumably taking place between the network of traffickers and the victims, with many receipts of funds occurring in 'wealthy' nations and few transfers to the areas of origin of the persons involved. Also of note was the frequent occurrence of such transactions in border areas where the migrants actually arrive, as well as in major cities, where the trafficking organizations are presumably centred. The subjective elements basically relate to the nationality of the remitters, who come from specific areas of Africa and the Middle East.

Trade in counterfeit goods

Another practice often noted in connection with money transfers is where the person making the transfer is both receiver and sender, with counterparties often located in different countries. One of the most frequent cases concerns remittances from North America to Italians and Africans located in the region of Campania, which are followed by remittances to China: these movements may be connected with the trade in counterfeit goods.

Operations with countries at high risk for money laundering

During 2017 the Unit continued its geographical and functional mapping of countries at high risk for money laundering.[74] An analysis of reports of suspicious transactions, backed up by evidence acquired through international cooperation, helped the Unit to identify a number of elements that make such countries attractive for potential money launderers: in some cases, it is because the true ownership of a company can be completely concealed, above all because bearer shares can be issued; in other cases, it is the low taxation or non-taxation of dividends and gains; in others again, it is the ease of setting up different types of company where monitoring tends to be more lax. In-depth analysis confirmed that some EU countries are also often implicated in the reports: because of the nature of their tax and company laws and the possibility to

[74] In these countries, which are traditional tax havens or offshore financial centres, the legislation favours tax arbitrage or guarantees the untraceability or secrecy of ultimate beneficiaries.

operate under the freedom to provide services, they may become a point of transit or arrival for funds of illegal origin.

Frequently, as a result of an attempt to take advantage of the options offered by several countries as well as to make it more difficult to trace transactions, single STRs will involve jurisdictions that allow opaque ownership structures and countries hosting major financial centres. An analysis of reports revealed that Luxembourg is used as a base for financial transactions involving complex corporate structures that often use trusts or vehicles set up in other high-risk jurisdictions, such as Guernsey, the Bahamas, the Cayman Islands or the British Virgin Islands. This system is often found in certain private equity transactions and can be used to transfer large financial flows of unclear origin to Italy.

Some interesting STRs revealed frequent transfers to Italy of funds from gaming companies set up in Malta; in most of these cases the money was withdrawn in cash. In-depth analysis of this type of STR brought to light a number of elements that, taken together, do not seem compatible with winnings from gaming. Notable features are the opaque ownership structures, the economic profile of the beneficiaries, the large amount of funds received within a short period of time, the withdrawal of cash and the use of pre-paid cards.

Video Lottery Terminals

As regards gambling, in 2017 the Unit again received several reports concerning video lottery terminals (VLTs). The reports flagged specific anomalies, such as excessively long gaps between ticket issue and re-use or collection, often following the same pattern and suggesting that the tickets could be used for the anonymous transfer of sums of cash. Although according to the Customs and Monopolies Agency these instruments are valid documents entitling only the issuers in connection with the underlying operation,[75] an analysis of the STRs suggests that the tickets are also used to transfer funds. Potentially, they can be issued for unlimited amounts, even after merely loading banknotes into the VLT without actually gambling, and can therefore easily be transferred between private individuals and used to settle any type of business, should people wish to conceal their economic reasons. In practice, they can be improperly used as banknotes, evading the legal limitations on the use of cash and with the additional advantage that they are easier to transfer physically (a ticket is smaller in size than a 5 euro banknote but can be worth much more) and the only disadvantage they have is that they must be cashed in within a certain period of time.[76] The new law on money-laundering has introduced 'speaking tickets' (containing information on how the value embedded in the ticket was formed and providing the licensee with evidence of the sums actually bet and won) which, once secondary legislation has been passed, will make it possible to identify any anomalous behaviour that may become the object of an STR.

Firms in difficulty and foreign special purpose vehicles

STRs submitted by professionals have been particularly useful in shedding light on some anomalous corporate operations undertaken by Italian nationals at the head of firms in evident financial difficulty and heavily indebted with the banking system. On

[75] See the decision of the Deputy Director of the Agency – Monopolies Section of 04/04/2017 which defines a 'ticket' as an 'entitlement to begin a game and/or to collect the nominal amount indicated, subject to validation by the gaming system'.

[76] The regulations require the recipient to be identified if the ticket is for an amount of €500 or more.

many occasions opaque special purpose vehicles (SPVs) were set up in non-transparent jurisdictions to make it difficult to trace the funds used to resolve the Italian firm's financial difficulties or, alternatively, to siphon off a large part of the capital before any arrangements with creditors were made. In the first case, analysis showed that shares in the failed Italian firm were sold to a specially created foreign firm, shielding the same owners, in order to bring funds illegally held abroad back into the country that were then used to repay the Italian firm's debts. In the second case, Italian nationals underwrote a capital increase of a foreign company via a trust in order to divert assets away from a pending bankruptcy procedure.

Property purchases by foreign nationals

There were also frequent reports in 2017 of very high value real estate transactions carried out in Italy by people from the former Soviet republics, often with a history of dubious economic activity in their home country or with family relationships with politically exposed persons. The analyses conducted brought to light certain recurring features, such as the geographical provenance of the subjects of the STRs, the purchase of luxury properties (often in exclusive locations), the frequent use of SPVs either owned by trusts or located abroad (e.g. in Malta or Cyprus) with accounts in third countries (Lithuania or Switzerland, and others), as well as funds transiting through accounts in the name of complicit professionals. The in-depth analyses benefited considerably from the insights obtained through contacts with other national authorities, which brought to light further anomalies relating to the same situations. This further confirmed suspicions that the operations described were designed to launder funds illegally acquired abroad by purchasing property in Italy.

4.2. The typologies

Below are some considerations relating to the three types of STR selected because of their frequency and connection with areas classified as high risk by the FATF and National Risk Assessment.[77]

4.2.1. Tax crimes

An analysis of STRs confirms that violations of tax regulations remained a versatile and transversal instrument in 2017 too, and one that was often used prior to re-introducing illegally acquired funds back into the system. In addition to STRs relating to conventional tax violations (organized into categories by the Unit, which has also drawn up indicators now widely used by reporting entities), during the year some reporting entities tended increasingly to notify tax violations involving a direct failure to make payments to the revenue agency. These violations were often part of broader fraudulent operations and were intercepted thanks to an increased awareness mainly on the part of the professionals involved, whose specific competences and privileged position give them access to information not normally available to other reporting entities.

In 2017 analysis revealed that tax crimes accounted for just over 24 per cent of total STRs, considerably less than in the previous year (about 36 per cent). This trend

[77] See the UIF Annual Report 2015, Chapter 1.

obviously reflects the drop in reports relating to voluntary disclosure, which represented about 27 per cent of the tax crime category (against 58 per cent in 2016).

A large part of this flow still pertains to the first version of the regularization process and hence relates to operations carried out following the repatriation of capital and generally involving anomalous use of the funds: this usually consists in transfers between linked physical and legal persons, investment in financial instruments and insurance policies and cash withdrawals. In-depth analysis focused on detecting possible improper use of the voluntary disclosure process and bringing to light any underlying money-laundering objectives.

Once again, the majority of the reports connected with the second voluntary disclosure procedure did not suggest any need for further analysis and for the most part stemmed from a notification of the client's participation in the voluntary procedure. The STRs varied in content in relation to the two types of phenomena characterizing the new VD procedure; they concerned, on the one hand, the extension of the deadline for the first procedure and, on the other hand, the introduction of a specific procedure for disclosure of cash and bearer instruments.

Again in 2017, in many cases the technical analysis of STRs that the Unit attributed to violations of tax regulations (false invoices, carousel fraud, sometimes international) revealed close links with organized crime or cases of usury, extorsion and corruption. Cash was often used in such operations.

As mentioned earlier, some reports were sent to the Unit regarding possible tax crimes involving failure to pay VAT or certified as withholding taxes.[78] The Unit forwarded the reported facts, along with the findings of the technical analysis, to the competent investigative authorities in accordance with Article 331 of the Criminal Code. STRs relating to tax crimes accounted for about 20 per cent of all reports forwarded under this Article and all were the object of further investigation. In some cases, the investigating authorities charged the offenders shortly after receiving the Unit's report.

The Unit's technical analysis revealed new irregular and criminally significant practices pertaining to the fiscal standing of tax contributors, specifically those related to tax credit transfers. A large set of financial operations containing elements typical of invoicing fraud may precede further criminal behaviour involving the assignment of tax credits, fraudulently generated via such operations, without observing the precautions dictated by the law.

The transversal nature of tax crimes and their role, alongside that of other anomalous behaviour, in broader criminal activity are borne out by the continued presence in 2017 of operations in which the improper use of invoices, as the ultimate fiscal document, made it possible to pursue illegal purposes other than the mere violation of tax laws. Examples are the issue of invoices for inexistent operations in order to obtain credit from banks or finance companies or their use to justify flows of funds to settle illegal transactions. In some cases suspicions were raised by the discovery that the persons or entities involved in the operation did not exist: the Revenue Agency has in fact provided the tools to verify, quickly and easily, whether the codes identifying

[78] See Chapter 3.5.2.

a 'tax subject' really exist.[79] Thus, commercial operations involving companies that no longer exist, even if still present in the companies' register, have sometimes triggered enquiries leading to STRs. The Unit's analysis then confirmed the possibility of tax crimes or potential fraud against financial intermediaries.

4.2.2. Corruption and misappropriation of public funds

Despite the very high risk, as outlined in the NRA in 2015 and often confirmed by news stories, the nature of the offences against general government makes it very difficult to develop preventive instruments as safeguards on a purely financial basis. Although such offences usually have financial repercussions, they take very different forms that cannot easily be grouped within a single, well-defined category. As a result, the preferred approach to tackling them is based on the prevention and monitoring of subjective aspects, partly in response to the changes in national and international regulations introduced in recent years. Thus, clients' public functions and political positions have become factors of risk that reporting entities need to monitor continuously by examining all operations and accounts involving them. Similarly, where such clients are involved in a reported operation, this may significantly affect the way an STR is handled by the Unit.

An examination of actual cases has shown, however, that although this approach is useful and often effective, it is not enough on its own to ensure that the matter is properly dealt with. There is no doubt that a thorough knowledge of clients' characteristics and a correct assessment of the flow of subjective information required to promptly intercept high-risk operations are essential for effective prevention. However, the findings of in-depth analyses, the outcomes of investigations and the contents of news reports have shown that financial transactions undertaken in pursuit of criminal purposes or in order to launder the associated profits do not usually involve politically exposed persons directly or any accounts in their name. It is therefore equally important, for the reporting entities monitoring those subjects, to examine the network of legal, economic and family relations carefully. The UIF is taking steps in this direction by developing tools that will make it easier, in the first stage of STR analysis, to identify situations where the involvement of politically exposed persons is not immediately apparent.

In 2017, some lines of enquiry launched the previous year were further pursued in collaboration with the investigative authorities and public prosecutors' offices, in parallel with analyses that revealed irregularities in the management of liquidation proceedings for public entities as mentioned in the 2016 Annual Report.[80]

These enquiries brought to light a complex network of companies and persons linked to specific economic centres or groups of companies providing consultancy or business services and with ramifications throughout the country.

[79] This is the portal on the Revenue Agency's website that can be used to check a tax code or VAT number.
[80] See the UIF Annual Report 2016, Chapter 3.5.1.

These groups worked in synergy using corporate accounts in which funds were deposited, as payment of invoices, by firms with links to general government and from which withdrawals were made for transactions with politically exposed persons that were entered as invoices for professional services or payment of shareholdings or various assets.

The analyses revealed that many of the companies belonging to the group under examination had ordered frequent transfers of funds in payment of invoices by firms involved in very large value administrative disputes, amounting to tens of millions of euros. In-depth analysis with the assistance of foreign FIUs revealed anomalous 'foreign-to-foreign' movements of funds between companies of the group and a person who had occupied important positions in the administrative justice system in Italy and had taken part in some of the multi-million euro disputes mentioned.

4.2.3. Operating typologies associated with organized crime

STRs possibly linked to organized crime generally do not contain elements that can be traced to specific forms of anomalous behaviour; this makes it harder to isolate them from other STRs in which the operations are outside the spheres of interest of criminal organizations. Thus, the subjective profile of the subjects of the STRs and the web of relations between them become central to the analysis. Accurately tracing that network in the course of in-depth analysis allows the investigative and judicial authorities to confirm (or refute) the links, elements and circumstances found during the enquiry.

In-depth analysis confirmed that criminal organizations have become highly sophisticated and work closely together to set up operations that will further their objectives, using financial products and services and complex legal structures alongside traditional methods. In this kind of context, a closer bond with legal and financial professionals as well as with the business world is fundamental, the long-term survival of which relies on mutual benefits.

The fund transfers reported can often be attributed to typical methods of false invoicing, although the operations are only theoretically consistent with the type of counterparties involved: the recurring use of bank accounts – often registered with foreign banks – for these fund transfers has sometimes made it possible to establish links between apparently unconnected series of operations.

An important issue that emerged during 2017 was the infiltration of organized crime into the crude oil and natural gas market, where ongoing problems at systemic level merit attention, owing to the size of the related financial flows and their cross-border nature, as well as to the fact that the observed behaviour may be linked to contraband in oil products. The operations uncovered, mainly aimed at tax evasion, ranged from fraudulent accounting of oil purchases and sales to companies operating in the same sector abroad, in both EU and non-EU countries: this involved triangulation with the final recipient of the goods (making it harder to trace flows of funds) by setting up fake export companies or firms providing false invoices to carry out carousel fraud schemes.

The flow of STRs recorded by operators increased as organized crime became more widely involved in the betting and gaming industry. In 2017, some STRs relating

to voluntary disclosure were also found among those directly or indirectly linked to organized crime (with the involvement of politically exposed persons).

Alongside the analysis of STRs, the Observatory on Organized Crime set up within the Unit continued to examine specific questions that had come to the fore as a result of the findings of investigations and judicial proceedings and of activity carried out in collaboration with various authorities to identify and trace anomalous financial flows in the name of figureheads or channels of finance used by organized crime. The Observatory's analyses helped to maximize the benefits of the UIF's database, providing an overview of various types of behaviour that share similar subjective features or relate to similar phenomena, and thereby improving our knowledge of the world of organized crime.

An initial study looked at the false ownership of assets, notably shareholdings, a method used by organized crime to launder illegally acquired funds through business activity. The focus was on defining specific indicators that might suggest false ownership through companies, making it difficult or impossible to recognize the effective ownership and trace any profits. The method adopted included selecting chamber of commerce data on economic sectors and geographical areas at a higher risk of criminal infiltration. Companies falling within this category were selected on the basis of qualitative and quantitative parameters (age of members of the firm, number of shareholdings or positions held by the same person, and so on). The positions identified by this means were found to correspond closely to the results of investigations, including those not relating to the cases reported, and confirmed that the method used was capable of identifying 'nominees' as a back-up to financial analysis.

Another study focused on areas at risk of tax fraud. The method developed used balance sheet data on reported firms to draw up a synthetic indicator capable of identifying companies issuing false invoices and occupying a central role in the network. Particular attention was paid to companies engaged in 'pure invoice fraud'– i.e. those with no production lines or organization, whose only purpose is to issue tax documents – which operate alongside firms that are effectively engaged in business. The starting point was the list of anomalies relating to invoice fraud circulated by the Unit,[81] which, together with evidence from the chambers of commerce, helped to create two complementary indicators, a quantitative one based on balance sheet data and a qualitative one relating to potential corporate anomalies (frequent moves of head office, changes of company name, suspicious events and so on).

[81] UIF Communication of 23 April 2012: 'Schemi rappresentativi di comportamenti anomali - Operatività connessa con le frodi fiscali internazionali e con le frodi nelle fatturazioni'.

5. COMBATING THE FINANCING OF TERRORISM

The terrorist threat has remained intense all over the world and taken on new and varied forms; there are terrorist organizations that control territories, organizations affiliated to complex networks, smaller cells and individual terrorists, all with different financing needs and sources. The international community has continued in its efforts to understand and monitor the most exposed channels, to check that traditional safeguards and their scope of application are suitable and to share information and experiences, on the understanding that only full agreement on objectives and close cooperation between States can provide appropriate prevention.

Mindful of this, the UIF is committed to refining its prevention system. Cooperation with the investigative bodies and the judicial authorities has continued to be intense as regards requests to the Unit for financial analysis as part of investigations or proceedings involving acts of terrorism; there have been several exchanges with the corresponding foreign authorities.

5.1. Suspicious transaction reports

The number of terrorist financing STRs has increased considerably since 2015, in connection with the upsurge in the phenomenon, mainly linked to the activities of ISIL in the occupied territories and to the numerous terrorist actions that have occurred in Europe too, carried out by local persons or cells connected with ISIL or individuals following radical ideologies (lone wolves) or 'foreign fighters'.

In 2017 there were nearly 1,000 reports on suspected terrorist financing from obliged entities, a growth of around 58.5 per cent compared with 2016 and ten times higher than the number received in 2014. In the same period, the share as a percentage of the total reports sent to the UIF went from 0.1 to 1.0 per cent.

Table 5.1

Terrorist financing STRs

	2013	2014	2015	2016	2017
Number of reports	131	93	273	619	981
Year-on-year percentage changes	-23.4	-29.0	193.5	126.7	58.5
Share of total reports	*0.2*	*0.1*	*0.3*	*0.6*	*1.1*

Two main factors have influenced these trends. The first is the greater awareness of obliged entities and the actions they have undertaken regarding the automatic detection and the analysis of suspicious movements and behaviour potentially linked to terrorist activity. The second is connected with more frequent activity on the part of the institutions: more intense prevention and suppression efforts in Italy by the authorities responsible, similar to what is happening for other significant crimes that cause public alarm, have given rise to STRs from operators with whom the subjects in question, or

people affiliated with them, have financial relationships or have worked, even if only occasionally.

The increased responsiveness of reporting entities has also been influenced by awareness-raising schemes adopted by the UIF by means of specific Notices on the subject, together with public interventions and meetings with the main operators.

The Notices released by the UIF have given rise to a growing number of reports which are likely to increase further with the gradual implementation of the indicators into the automatic STR detection systems of intermediaries.

Territorial distribution

The territorial distribution of reports in some cases reflects the greater presence of immigrants from ethnic groups that are generally perceived as being more involved with terrorism: about 30 per cent of reports involve transactions made in the province of Lombardy, a share that rises to 70 per cent in the regions of Veneto, Emilia Romagna, Piedmont, Lazio and Sicily.

About 37 per cent of the total of terrorist financing STRs were sent by the Payment Institutions category, especially by money transfer operators (the overall figure for the category's reports is below 10 per cent); the remaining reports, except for a small number of cases, are attributable to banks.

The most frequently reported transactions are cash deposits and withdrawals (34 per cent), followed by domestic credit transfers (16 per cent) and foreign ones (10 per cent), transactions connected with the use of credit cards and prepaid payment cards (19 per cent) and money transfer remittances (17 per cent).

Characteristics of terrorism STRs

The subjective element in terrorism financing STRs is traditionally one of the main ones, and in many cases the only source for suspicion and the reason for making the report. The financial patterns of terrorism have some particular features that make it difficult to identify them. Financial flows are often of lawful origin; financial requirements, especially for subjects who act alone or for small networks and isolated cells, are generally modest and can therefore evade the automatic detection systems for anomalous transactions. Lastly, transfers can be completed by using untraceable payment instruments and/or alternative circuits to the official ones, such as Hawala, which is used extensively within some communities.

The most common case (around half of the cases in 2017) is that of reports in which suspicion is founded entirely on subjective elements, especially the involvement of customers or their relatives in acts of terrorism or religious extremism, which usually emerges from open sources, automatic monitoring systems or when the investigative authorities request information.

Reports triggered by subjective elements, although in certain cases may seem hardly relevant because of their limited financial importance, often contain traces and information not only of a financial nature, which are invaluable for investigations. They contribute to identifying subjects' profiles, interpreting behavioural dynamics and reconstructing relationship networks.

In 2017, the share of these reports increased, above all as a result of the contribution of some international providers of money transfer services who have launched specific schemes to systematically and globally reconstruct the transfer networks attributable to subjects involved in terrorist attacks and to activate the relative reporting flows to the FIUs concerned (over 300 reports in 2017).

A fair number of reports, triggered by subjective elements, originated in the automatic monitoring systems used by intermediaries to identify access to the financial system (attempts to set up accounts or transactions with customers) by subjects included on the international terrorism lists (UN/EU, OFAC).

A case which occurs quite frequently is that of reports referring to non-profit bodies and organizations generally involved with religious assistance and support for local immigrant communities. This type of report accounted for just under 10 per cent of the total in 2017.

Reports on this kind of organization arise from enhanced monitoring procedures set up by operators on financial accounts held by such organizations and by the relative representatives, partly based on the anomaly indicators published by the Bank of Italy in 2010.

The most recurrent cases include cash deposits or withdrawals, anomalous in their frequency or in the amounts, and domestic and foreign credit transfers, with natural persons or other associations, which do not seem to be attributable to association activities or to fund raising. In some cases, suspicion refers to the methods for financing associations that are newly formed or being set up. Anomalous movements are often justified as being collections for building and fitting out places of worship, through the purchase and renovation of properties. Suspicion may also be focused on persons connected with such associations or with the relative local communities, such as representatives, treasurers or religious figures.

The reports not included in the previous cases, around 40 per cent of the total, often originated in financial anomalies of a general nature, traced to suspicions of terrorist financing based on where the transactions took place.

In most cases there are anomalies in the movements of cash and in the use of prepaid payment cards (used for example as a means of transferring funds, with third parties adding money to the cards followed by cash withdrawals by the cardholders).

UIF analyses

Over the last three years the competent authorities have been strongly committed to further analysing new forms of terrorism and the related financial profiles, especially the methods and channels for financing ISIL and associated phenomena, such as foreign terrorist fighters.

For the analysis of STRs, the UIF's analysts use all the information to which the Unit has access, not only of a strictly financial nature, together with network analysis techniques oriented towards investigating transfer networks, including complex ones. The analysis methods and pathways, though similar to those for examining cases of money laundering, are oriented above all to making the best use of the subjective information, the financial connections between subjects and any behaviour or financial trail, of however little importance, that might be useful inasmuch as it corresponds to the indicators described above.

The idea is to expand the initial information base by searching for signs and clues that could be promising from an investigative point of view, both to identify new cases and to reassess those already known to the investigative authorities. Financial trends are a primary source of information for interpreting behaviour, reconstructing movements and identifying terrorist networks, and can supplement traditional investigations.

The financing of terrorism through cross-border motor vehicle trade

One kind of report arising from suspicions of financing of terrorism is that involving the cross-border trade of motor vehicles, an economic sector whose possible connection with terrorist organizations – long recognized at international level[82] – has recently been confirmed by news reports on investigations in this area.

These investigations have shown how in most cases cross-border motor vehicle trade is used as the 'intermediate phase' in the chain of financial transfers that sustain terrorist organizations, in order to disguise both the end use and the origin of the funds, based on the following operational scheme:

- the funds, usually in the form of cash, are spent on purchasing used motor vehicles in countries where operations of this kind are easier (usually because the upper limit on cash transactions is higher than the price of the motor vehicle);
- the vehicles are resold several times among parties in various countries, with the subsequent transfer of the goods from one country to another;
- the buyers often include import-export firms which, at the end of the chain, sell the vehicles to counterparties located in jurisdictions lacking in anti-money laundering safeguards, so that it is easier for them to transfer the proceeds of the sales to countries at risk where the terrorist organizations to be financed are based.

In this series of operations[83] – given the anti-money laundering safeguards and the thresholds in force on the use of cash – it is mainly transactions in the second phase that are carried out in Italy since, if they are considered separately from those in other jurisdictions, they cannot be distinguished from ordinary sales transactions. For reporting intermediaries, therefore, suspicions of terrorist financing can arise from other circumstances such as countries at risk recurring among the destination countries for such flows or being where the parties settle/come from, regardless of the possible emergence of other profiles of objective anomaly which – given the phenomenon in question – may typically take the form of carousel fraud (intra-Community VAT evasion).

More recently, investigations have shown how cross-border motor vehicle trade (especially in used cars) can be used by terrorist organizations not only as a source of financing. Networks for smuggling migrants[84] actually use car dealers or import-export firms to justify their owning several motor vehicles for the clandestine transfer of immigrants, possibly even ex-foreign fighters, to their destination countries. In this case, a specific suspicion in connection with terrorism may arise following the recurrence of risks of a geographical nature or of subjective links with organizations or individuals close to radical environments.

---

[82] The FATF report "Emerging Terrorist Financing Risks" includes motor vehicle trade among the techniques classified as 'traditional'.

[83] For a more detailed description, see case No. 10 in Criscuolo C. et al., (2016), "Casistiche di riciclaggio e di finanziamento del terrorismo", UIF, *Quaderni dell'Antiriciclaggio*, *Collana Analisi e studi n. 7*.

[84] See the UIF's Annual Report of its work in 2016, specifically the box 'Analysis of migrant smuggling', page 52.

5.2. Information and support for reporting entities

UIF Notice of 13 October 2017

In its Notice of 13 October 2017, the Unit drew the attention of the obliged entities to the risk of considerable inflows to western countries of returnee terrorists, who are trained in the use of weapons, radicalized and whose movements are difficult to monitor. These subjects may provide logistical or executive support to terrorist initiatives in Europe and contribute to creating and organizing local cells and cross-border networks in the destination countries.

The notice - which in light of the growth of the terrorist threat provides additional elements to the Unit's previous Notice of 18 April 2016 - is based on the results of STR analysis, the evidence collected and further analysed in international forums and the comparison of experiences with foreign counterparts. The aforementioned cases do not indicate suspicious situations when considered individually, but their recurrence makes it necessary to carry out further integrated analyses that take account of all the information acquired.

The initiative is designed to raise the awareness of obliged entities and their staff as much as possible, on the assumption that they can play an essential role in detecting behaviour in clients that points to their religious radicalization, enabling a more precise contextualization of anomalous elements traceable to possible cases of financing of terrorism.

It is especially aimed at money transfer operators. Importance is also given to operations that transit on correspondent accounts and similar relations with counterparties based in countries or areas at geographical risk, to deposits of cross-border origin and to consumer loans not for specific goods or services, especially when they are immediately monetized or in the event of missed instalment payments.

Assessing geographical risk has underlined the need to consider: countries and areas affected by conflict, neighbouring areas and transit zones; countries that finance or support terrorist activities or where terrorist organizations operate; and jurisdictions lacking in safeguards for preventing and combating the financing of terrorism.

Where activities involve more than one intermediary or obliged entity (such as the transfer of funds), it is very important to ensure the ready availability of information within a business organization but also the transversal sharing of information on detected threats, in accordance with the AML decree.[85]

5.3. Action at international level

The FATF continued with its initiatives for monitoring the risks of terrorist financing in order to take account of the rapid evolution of the phenomenon and recognize the need to strengthen the mechanisms for preventing and combating terrorism, as part of the overall 'Strategy on Combating Terrorist Financing' and its 'Operational Plan'.[86]

[85] Article 39 (3) of Legislative Decree 231/2007.
[86] See Annual Report of the UIF on activities carried out in 2016, Section 1.2.

In 2017, the FATF's Recommendation 5 was revised and the standards for preventing the use of non-profit organizations for illegal purposes were updated, specifying the need to assess the exposure to risk of various types of organization analytically and thus to tailor the obligations and controls in terms of their effectiveness and proportionality. The UIF has continued its efforts to recognize updated forms of terrorist financing based on the operational experience of the national authorities.

In conjunction with similar analyses that FIUs carry out within the Egmont Group, there has been a focus on one hand on developments in ISIL financing, involving the exploitation of the resources of the territories it controls and of its foreign affiliates, and on the other hand on the detection of economic support for individuals fighting in conflict zones or returning to their country of origin following ISIL's retreat from occupied areas. Whether it is for logistical support or the organization of propaganda activities or the commission of violent acts in the destination countries, the financing of returnees is particularly varied and fragmented, and difficult to detect.

In order to take account of the developments in this area, the FATF has further investigated the forms of economic support for recruitment purposes. A specific FATF Report[87] also examines the ways for financing propaganda schemes that promote radicalization and affiliation by means of specifically designed materials and forms of communication, and highlights how this process is sometimes organized to make use of special channels for financial support.

Strengthening cooperation between authorities

The FATF project on 'Domestic Inter-Agency CTF Information Sharing', launched in 2016 as part of the 'Strategy on Combating Terrorist Financing' and completed in June 2017, focused on a comparative analysis of national systems, bringing to light problems in inter-institutional cooperation mechanisms, examples of best practice and indications for improving domestic models.

The FATF report highlights the need to expand the information sources available to the competent authorities for preventing and combating terrorism. It is fundamental for authorities, including the FIUs, to have access to investigative data relating to court orders, ongoing investigations and proceedings (including information on precautionary and confiscation measures), and to subjects 'monitored' by police forces or intelligence agencies or subject to an expulsion order. The Report also underlines the need to broaden the range of financial information available to the FIUs and to extend the access to administrative archives such as those for vehicle ownership, air and other forms of travel, and personal data regarding residency and family relationships.

There have been wider-ranging interventions in Europe, where a specific Directive[88] has extended the parameters of terrorism to include recruitment, training and travel in order to carry out or prepare terrorist acts. The Directive has also set out a broader definition of 'funds' that comprises a long list of goods with an economic value

[87] FATF, Financing of Recruitment for Terrorist Purposes, 2018.
[88] Directive (EU) 2017/541.

and extends economic support to include all the new types of behaviour that constitute the basic crime of terrorism.

The European Commission has also continued its commitment to setting up a European information system that centralizes data on transfers and payments to support analyses and investigations of cases of terrorist financing (EU Terrorist Finance Tracking System, EU TFTS). This is a similar instrument to the Terrorist Finance Tracking Programme (TFTP), set up in the United States shortly after 11 September 2001, which aims to broaden and facilitate access to financial information by the competent authorities.[89]

In 2017, the Commission began a feasibility study, collecting information on the national systems for gathering and using financial information, and assessing the options for setting up the EU TFTS. As part of the consultation of the member states, the UIF made a contribution by recalling the need for access to the system to be allowed in full, not only to the investigative authorities but also to the FIUs in order to support their analyses.

5.4. International cooperation

The instruments for international cooperation between FIUs are highly oriented towards the need to increase the volume and exchanges of information for the prevention of terrorism.

The FIUs have continued their efforts to broaden the range of information to be used in carrying out analyses and searches in all the databases and information sources available in each country.

They have also continued to exchange information through practices based on automated mechanisms and multilateral information sharing procedures. Specifically, as part of the ISIL Project launched by the Egmont Group to analyse ISIL financing and the financial characteristics of foreign terrorist fighters, a group of FIUs, including the UIF, continue to share information multilaterally on persons and activities of potential interest, in line with the aforementioned criteria.

Since the usual requests for information, based on descriptions of the case, grounds for suspicion and any links to the recipient FIU's country, are scarcely compatible with an effective preventive approach, continuous flows of information are necessary, which can be activated automatically on persons and activities that could be of interest (usually payments and fund transfers). In addition, to ensure timeliness and to expand the scope of cooperation, such exchanges often do not require unambiguous links with the FIUs in the countries involved or specific elements of suspicion. This 'intelligence-based' approach makes it possible to analyse and match data for the prevention and detection of activities of interest, anticipating the awakening of

[89] The 2010 EU-US TFTP Agreement established methods for cooperation between European and American authorities for TFTP data exchanges. Europol is tasked with regulating access to information by national organizations. Based on the consent of the competent Europol national Unit (ENU), some FIUs have access to the system, although the UIF does not.

suspicion based on specific facts which, in the absence of precise territorial references, take on a multilateral dimension.

The UIF now systematically uses an intelligence-based approach and, with the consent of the foreign counterparts concerned, it shares information and analyses with the competent national authorities so that it can better identify and locate persons involved in terrorism or the financing of terrorism. The UIF, in turn, helps the other FIUs participating in the project by sending unsolicited reports and providing evidence on the persons named in the reports it receives.

This kind of exchange has helped the UIF to share a huge amount of information on international remittances and other related networks that may be traceable to financial support for ISIL. Some 164 information exchanges were conducted in 2017, referring to more than 10,000 persons, a decrease of around 70 per cent compared with the previous year, attributable to changes in the phenomenon and context, characterized by the growing political and territorial weakening of the Islamic State, and to the need to shift the focus to restricted financing channels involving returnees and to recruitment and proselytizing activities carried out in Western countries.

6. STRATEGIC ANALYSIS

The international standards set by the Financial Action Task Force (FATF) and the Egmont Group consider strategic analysis to be one of the FIUs' official duties, together with operational analysis to investigate suspected cases of money laundering or the financing of terrorism. In keeping with these principles and with national legislation entrusting it with the analysis of financial flows for prevention purposes, the UIF is working to identify and assess phenomena, trends and system vulnerabilities.

The UIF's strategic analysis draws on the information and the indications obtained through the analysis of suspicious transaction reports (STRs) and aggregate data and any other relevant findings available to it. The data are processed and combined to help guide the UIF's action, the planning of its activities and the selection of priorities to pursue.

All UIF staff members contribute to strategic analysis, drawing on the wealth of information available, and enriching it with input from external sources, both open and confidential. The analysis rests on two pillars: the identification of typologies and patterns of anomalous financial conduct,[90] and the observation and study of financial flows and money laundering,[91] as discussed in this chapter.

An additional purpose of strategic analysis is to assess the risk of money laundering or the financing of terrorism involving the entire system or specific geographical areas, means of payment and economic sectors. By defining risk levels, the UIF can develop its own picture of the threats to and the vulnerabilities of Italy's anti-money laundering (AML) system. The UIF draws on the results of its strategic analysis when it participates in the preparation of the National Risk Assessment.

By picking out situations and contexts requiring ad hoc targeted enquiries, strategic analysis helps the UIF make informed decisions about its priorities.

The analysis also employs quantitative methods, such as econometric techniques and data mining tools, to identify trends and statistically significant anomalies. The most appropriate methodologies are chosen for each case, depending on the trend being examined, the data available and the preselected objectives. Quantitative techniques are particularly suited to analysing large masses of data because they can combine all the important information needed to study the variables of interest.

The dataset used by the UIF includes the aggregate AML reports (SARA) and information gained from operational analysis, cooperation with national and international authorities, and inspections. If needed, additional data and information may be specifically requested from financial intermediaries.

The main sources of information used by the UIF include the Bank of Italy's databases, which also contain data reports provided for prudential oversight purposes, and the Central Credit Register. Commercial and open databases are widely used as well.

[90] See Chapter 4.
[91] Article 6(4)(b) and (7)(a), Legislative Decree 231/2007.

6.1. The aggregate data

The analysis of financial flows carried out by the UIF is based mainly on the above-mentioned SARA reports. The data are submitted monthly by financial intermediaries, aggregating all the transactions carried out[92] according to the criteria set by the UIF in its own measures:[93] they include all transactions made by customers for a value of €15,000 or more (even if split up into different transactions). The SARA data are aggregate and anonymous and cover the entire spectrum of payment instruments and financial transactions.

In many countries, value-based reports, especially those referring to specific categories of operations, such as cash transactions, must be filed with the FIU, irrespective of any grounds for suspicion.

The main aggregation criteria for SARA data are mostly the type of payment instrument used, the location of the reporting branch, the customer's business sector and residence, and the location of the counterparty and of the latter's financial intermediary (in the case of wire transfers). Both inward and outward transactions are reported; the share of each transaction liquidated in cash is indicated separately.

SARA data

In 2017, the number of SARA data records sent to the UIF continued to rise as did the value of the underlying transactions (100 million records and 320 million transactions, an increase of 2 and 3 per cent respectively). The total amount, about €29 trillion, has increased significantly (by 30 per cent), mainly as a result of the new anti-money laundering decree. The relative share of the banking sector remained the same (95 per cent of the data records submitted and 97 per cent of the amounts reported). The number of reporting entities diminished slightly over the year (-3 per cent), mainly due to numerous mergers and acquisitions in the sector (see Table 6.1).

The effects of the new anti-money laundering decree

The entry into force of the new anti-money laundering decree in July 2017 had immediate repercussions on SARA data flows. The number of transactions reported and their total value increased as a result of the removal of exemptions from recording and storing the details of transactions made by customers under the simplified due diligence regime, such as resident financial intermediaries (or equivalent entities),[94] according to the previous anti-money laundering decree.[95] Following the new regulations, some intermediaries have started to record, and then transmit to the UIF as part of the aggregate data, the transactions made by customers comprising banking and financial intermediaries resident in Italy, the EU or equivalent countries.

Banks, asset management companies, and investment firms recorded larger increases in terms of the amounts reported (up by 30, 9 and 6 per cent respectively), while there was a large reduction in the reports made by payment institutions, down by 45 per cent on the previous year.

---

[92] See Article 33 of Legislative Decree 231/2007, as amended by Legislative Decree 90/2017.
[93] UIF Measure of 23 December 2013 on the transmission of aggregate data (only in Italian).
[94] The term 'equivalent countries' is defined in the Ministry of Economy and Finance Decree of 10 April 2015.
[95] See Section 1.3.1.

Table 6.1

Aggregate anti-money laundering reports (SARA data)

2017

Type of financial intermediary	Number of reporting entities	Total number of aggregate data records[1]	Total value of aggregate data records (billions of euros)	Total number of transactions underlying the aggregate data
Banks, Poste Italiane and CDP	634	96,700,981	28,042	301,080,172
Trust companies[2]	262	178,857	107	722,034
Asset management companies	188	1,687,512	255	7,586,182
Other financial intermediaries[3]	194	1,258,717	266	4,232,098
Investment firms	121	188,835	105	4,836,697
Insurance companies	80	1,397,496	126	2,660,940
Payment institutions	58	642,937	41	7,387,268
Electronic money institutions	6	5,237	1	211,195
Total	**1,543**	**102,060,572**	**28,943**	**328,716,586**

[1] The basic item of the SARA data report is calculated by the reporting agency by grouping single transactions according to precise criteria. SARA data can be rectified by the reporting entities; the statistics given in the table are based on data as at 13 March 2018.
[2] Includes the trust companies referred to in Article 199 of the Consolidated Law on Finance and in Law 1966/1939.
[3] The category includes financial intermediaries entered in the register pursuant to Article 106 of the Consolidated Law on Banking and in the special register referred to in Article 107 of the same law under the legislation in force before the changes introduced by Legislative Decree 141/2010.

The UIF provides continuous support for reporting entities: in 2017 it received around 2,000 email requests for assistance.

Cash transactions

Within the SARA database, information on cash transactions is of the utmost importance for preventing money laundering (as also signalled by the large number of STRs concerning the use of cash).[96] In addition to money deposited and withdrawn from current accounts, the SARA data also includes the amounts settled in cash in connection with other types of transactions, such as the sale of securities and issues of certificates of deposit.

The downward trend in cash transactions, noted in previous years' SARA data, continued in 2017, albeit more slowly (-2.1 per cent).

Not only is the decline a reflection of natural factors such as changes in purchasing behaviour and the greater availability and accessibility of electronic payment technologies, but it is also the result of the internal control mechanisms used by financial intermediaries and of the actions of the authorities to intercept and discourage illicit uses of cash. Italy is still, nevertheless, one of the countries in Europe with the highest level of cash use.[97]

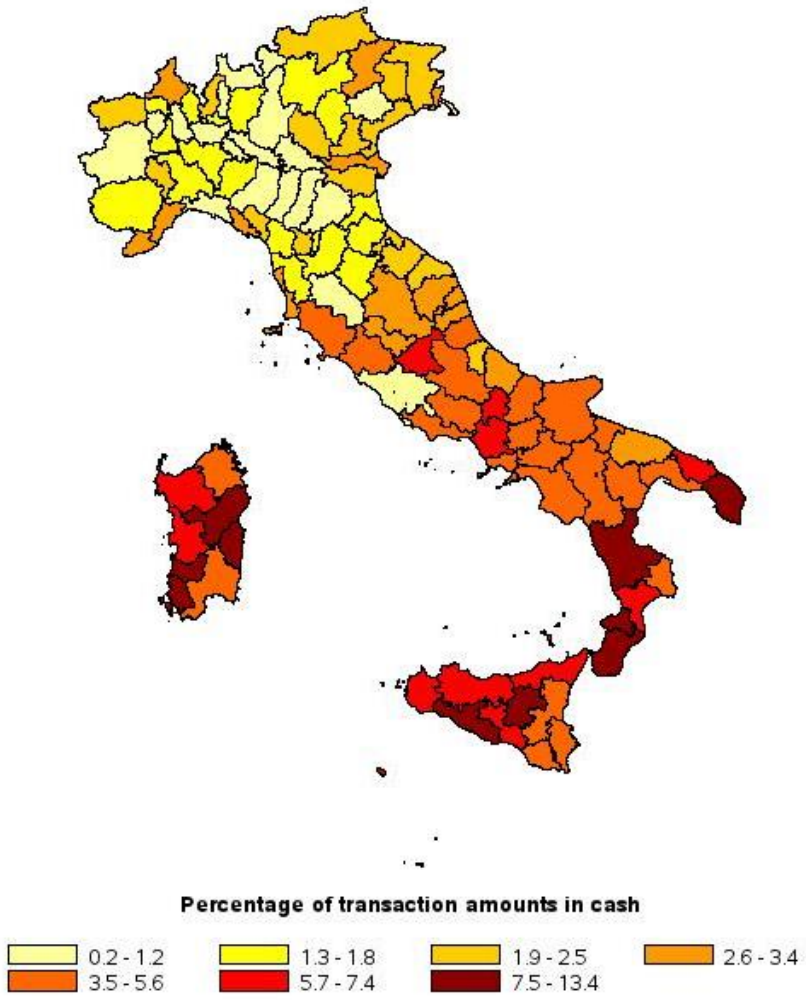
[96] See Section 3.2.
[97] See H. Esselink, L. Hernandez, (2017), "The use of cash by households in the euro area", ECB *Occasional Paper Series*, 201.

There was no change in the wide gap between total cash sums credited (€196 billion) and debited (€14 billion) according to the SARA data: withdrawals, which are typically split up into different transactions, tend to fall below the reporting threshold.

The geographical distribution of cash use (measured by share of total transactions) is still uneven (Figure 6.1): it is generally lower in the Centre-North (less than 4 per cent) and higher in the South and Islands (more than 13 per cent).

Figure 6.1

Use of cash by geographical area
2017



Note: Excludes transactions by general government entities and domestic/EU banks and financial institutions, or those resident in countries deemed equivalent under the Ministry of Economy and Finance Decree of 10 April 2015, for uniformity with the pre-existing rules. SARA data can be rectified by the reporting entities; the data used in the figure are updated to 13 March 2018.

Geographical differences in the use of cash are largely due to structural factors related to local socio-economic conditions, a preference for different payment instruments, and to the availability of financial services and how well they function. Nevertheless, a significant use of cash that cannot be explained by economic factors

may indicate illegal behaviour. This aspect is examined in a study published by the UIF in 2016, which presented an analysis of anomalous cash use at local level.[98] The results of the study led to the construction of geographical risk indicators, which are used in the UIF's institutional work and made available to the reporting entities, other authorities, the scientific community, and the public.

Credit transfers to and from foreign countries

Credit transfers are another payment instrument recorded in the SARA data that are of particular importance in the effort to counter financial crime. The credit transfer reports contain ample information, including details of the municipality (or foreign country) of residence of the counterparty and of the bank involved. Thanks to the large quantity of data, it is possible to compile statistics and make correlations based on the geographical origin and destination of the funds.

Of particular interest are the cases in which the foreign bank making or receiving a transfer is located in a tax haven or non-cooperative country. The transfer of funds to these jurisdictions may be for reasons that are not strictly economic, but rather connected to the opacity of their fiscal and financial systems.[99]

Data on transfers to and from foreign countries have been the most affected by changes in the regulations during the year. Excluding transfers made by EU banks or residents in 'equivalent' countries (not registered under the previous rules), the number of transfers to and from foreign countries recorded in SARA during 2017 increased by 3 per cent compared with 2016: inflows amounted to €1,300 billion and outflows exceeded €1,200 billion.[100] Inflows and outflows by foreign country are presented in Figure 6.2.

The main origin and destination countries for credit transfers are still Italy's traditional European trading partners, the United States and Turkey. Turkey's share of inflows and outflows continues to grow. The non-EU countries listed under 'Other countries' include Russia, China and Hong Kong for transfers to Italy, while China and Hong Kong are among the main non-EU destinations for outward transfers.

---

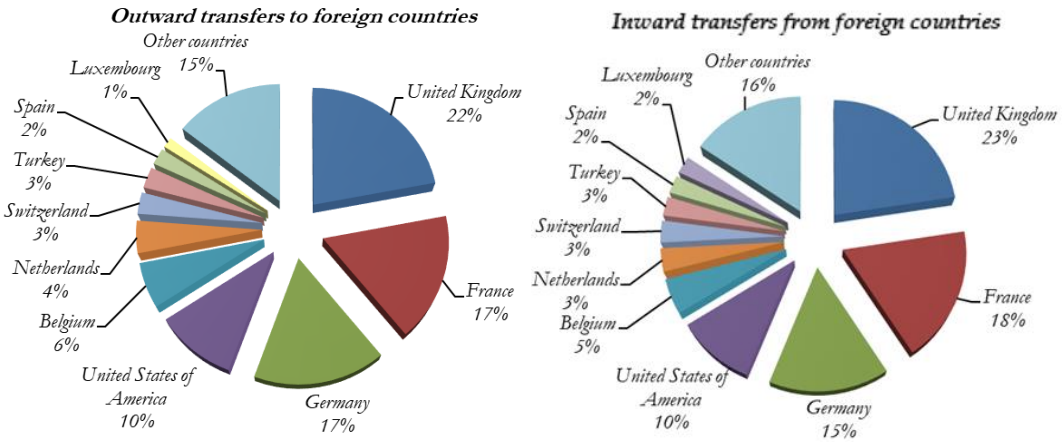
[98] Ardizzi G., De Franceschis P. and Giammatteo M. (2016), "Cash payment anomalies and money laundering: An econometric analysis of Italian municipalities", UIF, *Quaderni dell'Antiriciclaggio*, *Collana Analisi e studi n. 5*. See the UIF Annual Report for 2016, p. 78.

[99] For econometric evidence on outward flows and on the correlation between these and, respectively, the opaqueness of the destination country for the funds, see Cassetta A., Pauselli C., Rizzica L., Tonello M. (2014), "Financial flows to tax havens: Determinants and anomalies", UIF, *Quaderni dell'antiriciclaggio*, *Collana Analisi e studi*, 1.

[100] This sum excludes transactions by general government entities and domestic/EU banks and financial institutions, or those resident in countries deemed equivalent under the Ministry of the Economy and Finance Decree of 10 April 2015, in order to align it with the record keeping rules and the simplified due diligence in force at the start of the year. Since some reporting entities, in advance of the new anti-money laundering decree, had begun to record the transactions of such customers as early as the end of 2016, the annual changes presented do not take account of these transactions in either the current or the preceding year.

Figure 6.2

Credit transfers to and from foreign countries
2017



Note: Excludes transactions by general government entities and domestic/EU banks and financial institutions, or entities resident in countries deemed equivalent under the Ministry of Economy and Finance Decree of 10 April 2015, for conformity with the pre-existing rules. SARA data can be rectified by the reporting entities; the data used in the figure are updated to 13 March 2018.

Flows to and from tax havens

Credit transfers to and from tax havens or countries that do not cooperate in exchanging information for crime prevention or judicial reasons have always been worthy of special attention as regards money laundering prevention. The reference lists for these countries did not change significantly in 2017;[101] overall the flows to and from these jurisdictions have remained virtually unchanged, with just a slight increase of 1 per cent for inflows and 3 per cent for outflows.[102]

The flows to and from the main countries are detailed in Figure 6.3. There is still a very high concentration of credit transfers in a small number of counterpart countries: 90 per cent of the flows involve seven countries: Switzerland, Hong Kong, Abu Dhabi, Singapore, Monaco, Taiwan and Dubai.

In 2017 Iran became one of the top ten counterpart countries: credit transfers directed to this country doubled and there was an even greater increase in inflows from Iran. This trend can be ascribed to the increasingly visible economic effects of the changing political relations with Iran, resulting from the suspension of most of the financial sanctions.[103]

---

[101] The list of non-cooperative countries and/or tax havens included in the Glossary is taken from the ministerial decrees implementing the Consolidated Law on Income Tax (TUIR) that came into force on 31 August 2017, and from the list of high-risk and non-cooperative jurisdictions published by the FATF in February 2017, alongside the publication of the statistics in relation to 2017 in the UIF's Quaderni Antiriciclaggio, Collana Dati statistici. Compared with 2016, the following countries were removed from the list: Guatemala, Guyana, the United States Virgin Islands, Kiribati, Myanmar, New Caledonia, Papua New Guinea and the Solomon Islands. Ethiopia was added to the list in 2017.

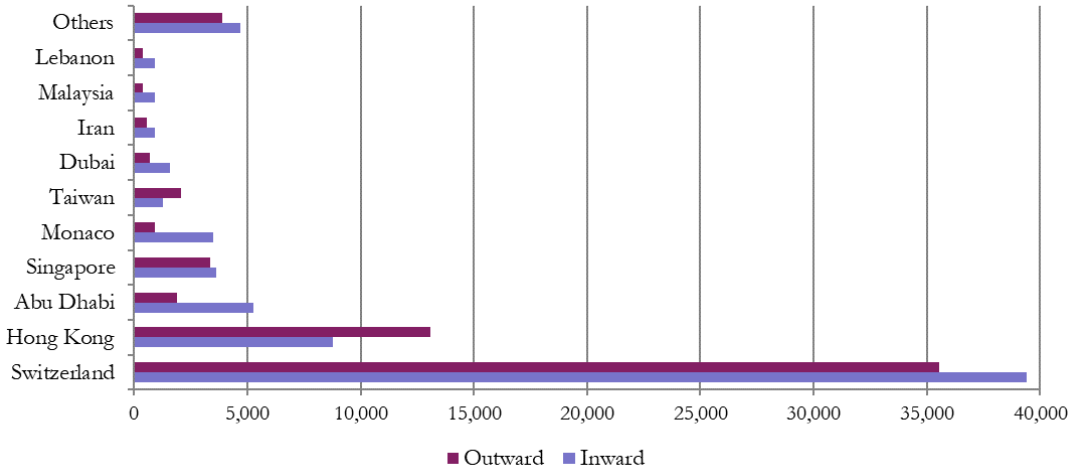
[102] To make a fair comparison between 2017 and 2016, for neither year were transactions considered that were made by domestic/EU banks and financial intermediaries or by those resident in 'equivalent countries', as defined in the Ministry of Economy and Finance Decree of 10 April 2015.

[103] See the UIF Annual Report for 2016, page 99.

Figure 6.3

Credit transfers to/from tax havens and non-cooperative jurisdictions (2017)

(millions of euros)



Note: Excludes transactions by general government entities and domestic/EU banks and financial institutions, or those resident in countries deemed equivalent under the Ministry of Economy and Finance Decree of 10 April 2015, for uniformity with the pre-existing rules. SARA data can be rectified by the reporting entities; the data used in the figure are updated to 13 March 2018.

By region

The geographical distribution across Italy of credit transfers to and from tax havens or non-cooperative countries is given in Table 6.2, which shows the usual differences: the regions in the north-west of Italy continue to originate and receive most of the transfers (66 and 59 per cent respectively), whereas the share of transfers involving the regions in the south of Italy and the islands is very small. The share of the central regions of the country has increased considerably as regards outward transfers (especially from the Lazio region), amounting to 17 per cent of the national total.

In order to assess and identify the presence of potentially illegal flows, a comparison can be made - for each combination of an Italian province and a foreign country - between the actual flows observed and the amounts expected on the basis of the economic, financial and demographic fundamentals of the provinces and countries involved. In this respect, the UIF conducts studies to identify suitable tools and models to detect such anomalies.[104]

[104] For further details, see Section 6.2.

Table 6.2

Credit transfers to and from tax havens and non-cooperative jurisdictions by region in 2017

	Outward transfers (millions of euros)	**% of total**	**Inward transfers** (millions of euros)	**% of total**
North-West	**41,636**	**66.3**	**41,546**	**58.6**
Liguria	1,417	2.3	1,993	2.8
Lombardy	28,906	46.0	33,361	47.1
Piedmont	11,274	18.0	6,134	8.7
Valle d'Aosta	39	0.1	58	0.1
North-East	**8,592**	**13.7**	**12,638**	**17.8**
Emilia-Romagna	3,677	5.9	6,171	8.7
Friuli-Venezia Giulia	607	1.0	703	1.0
Trentino-Alto Adige	440	0.7	654	0.9
Veneto	3,868	6.2	5,110	7.2
Centre	**10,915**	**17.4**	**12,790**	**18.0**
Lazio	7,595	12.1	4,239	6.0
Marche	556	0.9	838	1.2
Tuscany	2,558	4.1	7,482	10.6
Umbria	206	0.3	231	0.3
South	**1,380**	**2.2**	**3,362**	**4.7**
Abruzzo	155	0.2	1,926	2.7
Basilicata	18	0.0	34	0.0
Calabria	42	0.1	84	0.1
Campania	856	1.4	915	1.3
Molise	14	0.0	31	0.0
Puglia	295	0.5	372	0.5
Islands	**248**	**0.4**	**569**	**0.8**
Sardinia	35	0.1	184	0.3
Sicily	213	0.3	385	0.5
Total for Italy	**62,771**	**100.0**	**70,905**	**100.0**

Note: Excludes transactions by general government entities and domestic/EU banks and financial institutions, or entities resident in countries deemed equivalent under the Ministry of Finance Decree of 10 April 2015, for conformity with the pre-existing rules. SARA data can be rectified by the reporting entities; the statistics given in the table are based on data as at 13 March 2018.

Again in 2017, the UIF collaborated with the supervisory authorities and the institutions involved in preventing and combating money laundering by making targeted analyses based on SARA data.

6.2. Aggregate data analysis and research

Data quality is essential for ensuring the reliability of the analyses and studies of financial flows. To detect possible reporting errors, as soon as they are received by the UIF, the aggregate data undergo automatic statistical checks based on quantitative methods. This checking serves to identify not only possible data errors, but also any anomalous flows requiring further investigation by the reporting entity.

There are two types of controls: systemic checks, which compare the data of each reporting entity with those of the entire system for the same month; and non-systemic checks, which compare the conduct of individual financial intermediaries against their own reporting patterns over the previous 12 months.

The data identified as anomalous by the control algorithms are sent to the intermediaries so that they can check for mistakes themselves and correct any reporting errors.

Statistical controls on data accuracy

In 2017, checks revealed around 27,000 statistical anomalies in the aggregate data, which led to 906 reporting entities (including 579 banks) being questioned. In only a small number of cases did the intermediary correct the data (7 per cent of banks and 5 per cent of financial intermediaries). In 429 cases (2 per cent of the total), the anomalies detected by the controls involved STRs that had already been sent to the UIF. In another 255 cases, following a request for verification, the checks made by the intermediaries led to them considering whether or not to file a report.

The UIF develops its analyses of the phenomena and financial conduct of interest by making use of econometric techniques, with the twofold aim of increasing knowledge about specific phenomena and of providing operational guidelines for preventing and combating money laundering. The findings are used internally to identify sectors and geographical areas at risk and cases in need of closer scrutiny. The evidence is also shared with the other authorities that are part of the AML system according to their respective responsibilities. The methodology and general findings are published in the Quaderni dell'Antiriciclaggio, Collana Analisi e studi.

New study on foreign credit transfer anomalies

In 2017 there were more econometric analyses of financial flows in and out of Italy, in order to identify trends and anomalies. The map of anomalies of outward financial flows was updated to include the last few years, using the same methodology as that used in a previous study carried out by the UIF.[105] The latest study also extended the model to analyse inward flows. Credit transfers from each Italian province to each foreign country are compared against the volume of transfers expected on the basis of economic, financial and demographic fundamentals such as population, per capita GDP, foreign direct investment, distance from the foreign country, and the presence of immigrants. Financial flows at the province/foreign-country level whose volume is significantly different from what might be expected are classified as anomalous. A similar analysis was made of the flows of credit transfers received in each Italian province from individual foreign countries. The validity of this methodology is confirmed by the fact that the most anomalous inward and outward flows tend to involve, domestically speaking, the provinces with the highest crime rates and, externally, those countries with a higher risk of corruption or money laundering and more opaque as regards taxation, company law and finance.

[105] Cassetta A., Pauselli C., Rizzica L., Tonello M. (2014), '*Financial flows to tax havens: Determinants and anomalies*', UIF, *Quaderni dell'Antiriciclaggio, Collana Analisi e studi,* 1. The original study analysed the financial flows to and from other countries in the period 2007-2010, while the new study uses 2015 data.

Anomalous outflows were correlated with the size of the black markets for goods and services in the provinces of origin ('enterprise syndicate crimes'), while anomalous inflows were correlated with the strength of criminal control of the territory in the destination provinces ('power syndicate crimes'). A possible interpretation of these findings is that illicit funds flow out of the areas in which they are produced and are then sent back to where the real beneficiaries are resident, presumably travelling through less transparent jurisdictions to screen the origin.

Anomalous uses of cash

The refinement of the analysis model for cash anomalies was completed last year. The new econometric methodology produces money laundering risk indicators at a more detailed level than in previous studies and so it is now possible to further differentiate individual intermediaries within each Italian municipality.[106] In the future, this will lead to more detailed operating guidelines, which will help the UIF, the other authorities, and the reporting system to better prevent and combat money laundering.

Anomalous trade flows

The UIF and the Bank of Italy's DG for Economics, Statistics and Research have developed an empirical analysis of the discrepancies in the bilateral ('mirror') statistics on Italy's foreign trade in order to identify anomalous trade flows. The initial findings are encouraging as regards the capacity of this approach to detect flows that may be connected with the outflow of illegal funds from the country.

Anomalies in inward and outward trade flows: an analysis of the discrepancies in the bilateral statistics

For some time now, national and international anti-money laundering authorities have been looking at 'trade-based money laundering'. By exploiting irregularities in declarations and accounting, money launderers and criminal organizations use goods trade to transfer illegal funds from country to country; over-declaring the value of imports or under-declaring that of exports is one of the most commonly used methods for transferring illicit assets abroad.

One possible way, suggested by the literature, of detecting these anomalous flows is by comparing the bilateral ('mirror') statistics on foreign trade of counterpart countries.[107] Consistently with this approach, a model has been estimated in which the variable being analysed is the value of the discrepancies observed in the period 2010-2013 in trade flows between Italy and each counterpart country, at the most detailed level of product classification (6-digit, Comtrade-UN data).

This study has a higher degree of accuracy than those in the existing literature because, thanks to the Bank of Italy's Survey on International Merchandise Transport, the value of the imports can be shown net of transport costs. The explanatory variables include the structural factors of the discrepancies themselves, among which: the socio-

[106] Ardizzi G., De Franceschis P. and Giammatteo M. (2016), "Cash payment anomalies and money laundering: An econometric analysis of Italian municipalities", UIF, *Quaderni dell'Antiriciclaggio*, *Collana Analisi e studi, 5*.

[107] The value of imports to Country A from Country B in a given product sector and a given period is compared with the corresponding value of exports from Country B to Country A in the same sector and period in the context of their respective Balances of Payments. Excluding some technical factors and accounting conventions, the values should mirror each other.

economic characteristics of partner countries, the geographical distance from Italy, membership of the European Union, and the level of taxation.

Taking these factors into account, the model makes it possible to identify a component that may be attributable to false declarations, which can therefore be classified as 'anomalous'. On the basis of these flows, it was possible to produce risk indicators at country and macro-sector level. In line with what emerged in the literature, illicit flows tend to be concealed within ample and consolidated trade: countries with the highest incidence of anomalous flows include several of Italy's major trading partners.

The main result of this work is the identification of trade that may be connected with illegal flows, with highly detailed results at country and sector level. The preliminary findings on the model's ability to capture anomalies of interest for anti-money laundering purposes (even for more recent years than those of the estimation period) are encouraging: some of the most anomalous country-sector flows identified were confirmed by the information held by the UIF, which came from operational analysis work and from exchanges of information with other authorities.

Balance sheet analysis of infiltrated businesses

A study of the economic ownership and financial situations of companies infiltrated by organized crime, based on the analysis of balance sheet data, was launched in collaboration with the Special Operations Group of the Carabinieri. By focusing attention on a sample of companies controlled or infiltrated by organized crime and integrating the data in financial statements with information from other databases (for example, the Central Credit Register), the analysis aims to highlight recurrent factors in the structure, management, and operations of these companies.[108] In addition to increasing general knowledge about criminal infiltration in the economy, the project could lead to the construction of risk indicators to be used in the institutional activities of the UIF and which could possibly be disseminated in the interests of preventing and countering money laundering.

The specific evidence that emerges from research work and studies is increasingly being applied at an operational level. During 2017, the findings of two strands of analysis were examined further.

Anomalous cash withdrawals using foreign cards

The first concerns the monitoring of anomalous cash withdrawals in Italy by means of foreign payment cards.[109] As regards the most interesting cases, our foreign FIU counterparts were required to identify the cardholders. The evidence obtained confirmed that huge cash withdrawals made in Italy with foreign cards could be used to repatriate funds of illegal origin held or accumulated abroad. The results of the analyses and the information gathered were forwarded to the law enforcement agencies for follow-up work.

With reference to the 165 most suspicious cards, 20 FIUs were consulted, which led to 92 names being detected, 65 of which led to the discovery of important information; 29 of the latter had previously been reported to the UIF by Italian

[108] Infiltrated businesses were identified on the basis of various types of judicial proceedings (precautionary seizures and confiscation orders).
[109] See UIF Annual Report 2015, p. 74.

intermediaries. It emerged in some cases that the holders of cards issued by banks based in other European countries were Italian citizens involved in legal proceedings in Italy for various crimes (such as tax fraud and corruption; one nominee of a criminal organization was also involved). Other cards with 'significant' activity were held in the names of citizens of countries in Eastern Europe and the Middle East and were used in a coordinated way to make withdrawals in the areas surrounding Naples and Trieste.

Screening of flows at risk

A second line of operational analysis focused on positions of interest that emerged from the monitoring of financial flows directed towards Arab and North African countries.[110] Some SARA transfers with time inconsistencies in comparison with previous trends underwent detailed analysis using: extracts from the Single Electronic Archive (AUI) specifically requested from the intermediaries; the databases available to the UIF (STR archives, commercial databases); and the information provided by foreign FIUs. Here too, the findings that emerged in relation to possible suspicious financial behaviour were reported to the investigative bodies.

The positions of interest that emerged mainly concerned triangulations, in some cases passing through current accounts in correspondent Italian banks, which allow commercial supplies coming from one country (including Italy) to be paid by means of bank transfers directed to third countries, often characterized by elements of financial opacity.

Other activities

In 2017 the UIF once again participated actively in national and international academic debate on topics related to its activities. For the third year running, together with Università Bocconi, the UIF organized a workshop on quantitative methods to counter economic crime.

Third UIF-Bocconi Workshop on quantitative methods to counter economic crime

The UIF, in partnership with the Baffi-Carefin Centre for Applied Research on International Markets, Banking, Finance and Regulation of Università Bocconi in Milan, in October 2017 hosted the third edition of the workshop on 'Quantitative methods to counter economic crime'.

Besides looking closely at the models put forward in the scientific literature on financial crime, the workshop was mainly concerned with sharing the implications and operational potentialities of quantitative methods with the institutions involved in preventing and combating money laundering. In addition to the experts from the UIF and the teaching staff of the Università Bocconi, the workshop was also attended by Bank of Italy economists, other researchers and academic staff, and representatives of some government, law enforcement, and judicial authorities.

At the workshop, the UIF presented its study of anomalies in outward and inward foreign bank transfers and a model for estimating the illegal financial flows connected to international trade in goods, as described above. A researcher from Istat illustrated the methodology adopted to estimate the drugs market when compiling the national accounts; some economists from Università Bocconi and Università di Milano-Bicocca

[110] See Annual Report of the UIF on activities in 2016, p. 84.

presented local money-laundering risk indicators. A researcher from Università di Roma Tor Vergata presented the application of social network analysis techniques to an intermediary's Single Electronic Archive in order to create risk indicators linked to individual subjects and transactions.

Two contributions described the findings of the econometric analyses of the role played by criminal organizations in influencing election results and the behaviour and selection of politicians (one from Strathclyde University and York University, UK and the other from Università Bocconi, Italy).

Lastly, one workshop session was dedicated to the infiltration of organized crime into Italian businesses. An introductory econometric study (carried out by the Bank of Italy) looked at the effects of the infiltration of an organized crime group (the 'ndrangheta) on the performance of companies operating in the Centre and North of the country. A second study analysed the impact of organized crime on a sample of Lombard and Calabrian companies in order to identify the most common vulnerabilities (Università Bocconi and University of Miami).

The studies conducted by the UIF were presented at the annual meeting of the Società Italiana degli Economisti and at the annual conference of the Società Italiana di Economia e Diritto. In the international arena, the growth in the visibility of the strategic analysis carried out by the UIF was reflected in its participation in various scientific and institutional meetings: presentations were made to the Eurostat Task Force in Brussels on the measurement of criminal activities in national accounts ('Illegal Economic Activities in National Accounts and Balance of Payments') and to the 'Financial Crime 2.0' conference in London, organized by the British think tank RUSI - Royal United Service Institute. At a third meeting of experts in Vienna, organized by the UN Office on Drugs and Crime (UNODC) and the UN Conference on Trade and Development (UNCTAD), the UIF presented a paper on the construction of indicators of 'illicit financial flows', which is one of the areas for action set out in the UN's 2030 Sustainable Development Agenda.

6.3. Gold trade declarations

The law governing the gold market in Italy provides that transactions involving investment in gold or gold materials for mainly industrial uses (other than jewellery) should be declared to the UIF. This requirement applies to the cross-border trade or transfer of gold for amounts of €12,500 or more.[111]

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

There are two types of declaration: monthly declarations, submitted with reference to all transactions made in the reference period; and those submitted prior to

[111] Law 7/2000 and subsequent amendments.

a physical transfer of gold out of the country ('monthly declarations' and 'advance declarations').

Statistics on monthly gold trade declarations

The total number of gold transactions declared monthly to the UIF in 2017 declined slightly from just over 100,000 to around 96,000 (see Table 6.3). However, the quantity and overall value of the gold traded remained unchanged at about €13 billion, also given the substantial stability of the average annual listing. The growing trend in physical transfers of gold out of the country continued: in 2017 the number of advance declarations more than doubled from 53 to 137, while the amounts involved increased even more markedly from €13 million to €168 million. The transactions were mostly made by a small number of reporting entities.

Table 6.3

Declarations of monthly gold transactions
2017

Type of transaction	Number of declarations	Number of transactions	Declared value (millions of euros)
Sales	36,469	96,010	12,908
Gold loan (concession)	1,928	3,818	1,124
Gold loan (restitution)	500	572	67
Other non-financial transactions	110	110	87
Personal imports of gold	137	154	168
Transfer as collateral	0	0	0
Delivery services for investments in gold	533	541	158
Total	**39,677**	**101,205**	**14,512**

The number of reporting entities registered in the gold trade declaration system increased to 662 (see Table 6.4). The UIF provides assistance to the reporting entities both at the time they join the system and also when they have to produce and send in their declarations: 2,800 requests for assistance were received via email in 2017.

Table 6.4

Categories of reporting entities engaged in transactions in gold
2017

Type of reporting entity	Number of reporting entities registered	Number of reporting entities active in the year	Number of declarations [1]
Banks	84	48	7,766
Professional gold dealers	426	357	32,199
Natural persons	92	14	16
Private legal persons	60	24	658
Total	662	443	40,639

[1] Includes monthly declarations and advance declarations.

In 2017, the number of new registrations fell by almost half to 57 compared with 109 in 2016, mainly due to the reduction in the number of natural persons registering (53 in 2016, 17 in 2017).

Most of the transactions continued to be investments in gold (53 per cent) and industrial gold (40 per cent). Only a small amount (7 per cent) involved mixed transactions for which it is not possible to find a single purpose for the underlying transaction. The distribution by reporting entity of the amounts involved showed a slight increase in the share of banks (from 25 to 27 per cent) and a slight decrease in that of professional dealers (from 75 per cent to 71 per cent). The share accounted for by private individuals remained at around 1 per cent.

Italian counterparties

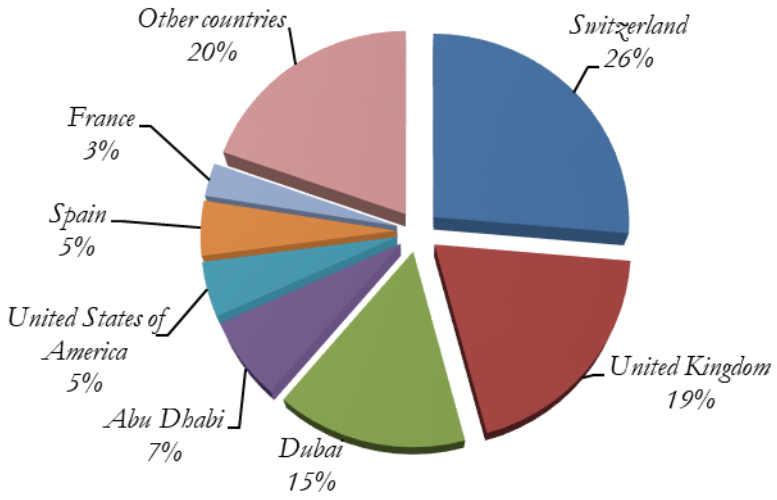
The geographical distribution of Italian counterparties remains highly concentrated, with Arezzo, Vicenza and Alessandria, which traditionally specialize in gold working, still accounting for 61 per cent of the market for the period, similar to the previous year.

Foreign counterparties

The value of transactions with foreign counterparties fell to €4 billion euros, down by 9 per cent on 2016, accounting for just under one third of all transactions. Transactions were still concentrated in just a few counterparty countries: the top five accounted for 72 per cent of the total (see Figure 6.4).

Figure 6.4

Gold transactions with foreign counterparties
2017



As regards composition, the group of the most important foreign counterparties remained essentially unchanged, except for the fact that the United States is now one of the top five, its share increasing from 1 per cent in 2016 to 5 per cent in 2017. Switzerland's share decreased again (from 28 per cent to 26 per cent) as did that of the United Kingdom (from 20 per cent to 19 per cent), while the increase in amounts transferred to and from counterparties in Dubai continued to rise (from 12 to 15 per cent) as it did, to a lesser extent, for those in Abu Dhabi (from 6 to 7 per cent).

Statistics on advance declarations of gold transfers abroad

Advance declarations are only for physical transfers of gold abroad, which must be submitted to the UIF before any gold crosses the border. If the gold is not being transferred to a new owner, the advance declaration is the only source of information for such transfer.

Advance declarations of cross-border physical transfers of gold declined compared with 2016 in terms of the number of transfers declared (-7 per cent), with a drastic reduction in the value of the gold transferred (-48 per cent; see Table 6.5).

Table 6.5

Advance declarations of transfers of gold abroad [1]
2017

Type of transaction	**Number of declarations/ transactions**	**Declared value** (millions of euros)
Sales	928	686
Unclassified	30	6
Gold loan (restitution)	4	0[2]
Total	**962**	**692**

[1] Advance declarations are included in the monthly declarations when they relate to commercial or financial transactions.
[2] The total amount declared for restitution of gold loans was €0.5 million in 2017.

The advance declarations almost always referred to gold being transferred abroad (99 per cent of the total value).

The UIF proactively checks the data and operations of entities registered with the gold trade declarations collection system. The anomalies that emerge are analysed further and the most interesting results are sent to the relevant law enforcement bodies.

The UIF collaborates with the competent authorities that work to prevent and combat crime, including in relation to data on gold trade declarations. In 2017, the UIF received 7 requests for information in this regard.

7. CONTROLS

7.1. Inspections

The UIF contributes to preventing and combating money laundering and the financing of terrorism in part through on-site inspections of entities subject to reporting requirements.[112]

An on-site inspection is a non-routine prevention tool used in conjunction with off-site assessments to verify compliance with the active cooperation obligations and to obtain important information on operations and phenomena. In general, on-site inspections are geared towards strengthening active cooperation and improving the quality of the reports submitted to the UIF.

The UIF conducts general inspections to examine at-risk sectors and operations more closely and to check that the procedures for reporting suspicious transactions are adequate and that the active cooperation obligations are being fulfilled. It also carries out targeted inspections to verify and expand upon specific information acquired during the analysis of STRs or received from foreign FIUs, or during the course of its cooperation with judicial authorities, investigative bodies and supervisory authorities for the sector.

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

In 2017, the UIF carried out 20 on-site inspections (see Table 7.1), of which 18 were general and 2 were targeted, concerning cash management measures at some cooperative credit banks.

Table 7.1

Inspections

	2013	**2014**	**2015**	**2016**	**2017**
Number of inspections	21	24	24	23	**20**

The planning of the general inspections for 2017 was focused on compliance as well as on gathering information and analysing new non-financial sectors, consistent with the preceding years.

The entities to be inspected were chosen on the basis of criteria which could be indicative of deficiencies in the areas of active cooperation or of increased exposure to the risks of money laundering and terrorism financing, namely: the absence or low

[112] Articles 6(4)(f) and 6(5)(a) of Legislative Decree 231/2007.

number of STRs; parties repeatedly mentioned in STRs transmitted by other obliged entities and in the information provided by investigative bodies or by sectoral supervisory authorities; missing aggregate data; and detrimental information concerning the reporting entity, or its customers, drawn from statements or public sources. The planning also took account of the coordination contacts with the sectoral supervisory authorities, the Customs and Monopolies Agency and the Special Foreign Exchange Unit of the Finance Police.

In the banking sector, checks were performed on private banking activities carried out by financial consultants. Weaknesses were found in the sharing of information on customers' personal profiles between the sales network and the AML function and in detecting more complex transactions carried out among related companies or entities. Active cooperation was negatively affected by excessive reliance on information provided by financial consultants. Disciplinary action against financial consultants for non-compliance with AML legislation rarely resulted in investigations for possible STRs.

General inspections at small fiduciary companies revealed critical issues in relation to: i) customer acquisition largely based on the input of third-party professionals without adequate safeguards against potential conflicts of interest; ii) IT systems that are unfit for the continuous monitoring of customer transactions; iii) failure to exploit all the information available or obtainable when processing an STR (e.g. information drawn from the requests made by investigative bodies in the context of their checks or investigations of customers); and iv) inadequate sharing of information regarding the reporting activities of the parent company as regards fiduciary companies in the banking sector.

Inspections of auditing firms revealed weaknesses in internal AML controls and in the analysis of customers' accounting data for active cooperation purposes.

In the insurance sector, weaknesses were found in fulfilling the obligations of due diligence and in keeping records, because the information shared between the sales points (often banks) and the central structures of the companies responsible for STRs was not always reliable. Areas of weakness concerned: i) the fragmentation of information on the personal profile of shared customers; ii) the absence of specific parameters for evaluating insurance activities (restrictions on policies) in the customer profiling process and shortcomings in the on-going monitoring of transactions; and iii) STRs that did not always contain all the data acquired during the preliminary filing process.

Inspections continued at EU payment institutions operating in the corporate and retail money service business (MSB).

In the corporate sector, the risks inherent in the service provided by payment institutions, which envisages their involvement in the transfer of funds, were underestimated, making the traceability of the parties involved in the transfer more burdensome. In the retail sector, IT procedures were not always adequate in ensuring the necessary timeliness in identifying the transactions to be subjected to CFT freezing measures.

Following inspections by the UIF and subsequent measures taken by the Bank of Italy, in September 2017 an EU payment institution whose Italian branch had shown

significant critical issues regarding compliance with sector regulations had its authorization revoked by the supervisory authority of its home country.

Inspections continued in the gaming sector, which is particularly vulnerable to the infiltration of funds of dubious origin or destination; the firms to be inspected were selected in cooperation with the Customs and Monopolies Agency.

The main critical areas in gaming over physical networks concerned the low propensity on the part of gaming licensees to evaluate irregularities in the management of distributors and operators, including for active cooperation purposes. The sector is exposed to significant risks, especially with regard to the use of video lottery terminals (VLTs). The risks associated with VLTs may be partly mitigated by the implementation of the new AML and sector legislation. For online gaming, difficulties remain in ensuring adequate controls on the traceability of reload and withdrawal transactions on gaming accounts.

In 2017, measures were launched on credit securitization transactions in the servicing sector, especially with regard to the non-performing loan compartment.

The inspections sought to reveal any critical issues pertaining to compliance with the reporting requirements, taking account of the high number of parties potentially involved in the financial flows associated with securitization transactions.

Based on the inspections carried out in 2017, the UIF transmitted to the judicial authority the required reports on evidence of possible criminal activity, initiated sanctions procedures for administrative violations, involved the supervisory authorities on the matters under their competence, and supervised the inspected entities regarding the detected shortcomings and the corrective measures to be adopted.

7.2. Sanctions procedures

The anti-money laundering regulatory framework envisages a complex system of administrative sanctions designed to punish violations of its obligations. The UIF ascertains whether there has been a violation of the obligation to report suspicious transactions and, depending on the violation, informs parties of the allegations against them and submits the alleged violation to the MEF or the sector's supervisory authority so that they may impose the sanctions envisioned under the law.[113]

Given the wide range of entities subject to reporting requirements, the sanction measures perform a significant enforcement and deterrence function, but are only complementary to those that derive from the overall system of organizational safeguards imposed by legislation, from the controls performed by various authorities and from the risks of a criminal nature.

The FIU calibrates its measures to the strategies adopted during inspections, highlighting the omissions indicative of a lack of attention to active cooperation and the risks of money laundering or the financing of terrorism.

[113] See Section 1.3.1.

In 2017, the FIU started sanctions procedures in 17 cases (11 following on-site inspections and 6 on the basis of off-site assessments) for failure to report suspicious transactions. These sanctions procedures were then assessed by the MEF for the imposition of a fine (see Table 7.2).[114] In all, the total value of these violations amounted to around €100 million.

During the same year, five sanctions procedures were conducted for violations of the obligation to freeze funds and financial resources in accordance with the law on the financing of terrorism;[115] specifically, the UIF initiated three procedures following inspections and, for the other two, the UIF carried out the investigation and transmitted its report to the MEF.[116]

With reference to the law on gold trading,[117] the UIF ran investigations and submitted reports to the MEF for five sanctions procedures in 2017 for failure to make the required declaration of transactions involving gold transfers or trades with a value of €12,500 or more.

Table 7.2

Administrative irregularities

	2013	**2014**	**2015**	**2016**	**2017**
Failure to report a suspicious transaction	29	11	32	17	**17**
Failure to transmit aggregate data	-	-	-	1	**-**
Failure to report a transaction in gold	7	8	7	5	**5**
Failure to freeze funds and financial resources	7	8	10	8	**5**

[114] This refers to procedures for violations that preceded the effective date of the reform of the AML legislation (i.e. 4 July 2017); procedures initiated after that date took into account the transitional regime provided by the reform.
[115] See Section 8.2.1.
[116] In accordance with Article 31 of Decree of the President of the Republic (DPR) 148/1988, referenced in Article 13 of Legislative Decree 109/2007, in force on the date of the alleged violation. With reference to the sanctions procedure, Legislative Decree 109/2007, as amended by Legislative Decree 90/2017, no longer refers to the Consolidated Law on Foreign Exchange Regulation (DPR 148/1988) and contains a specific provision (Article 13-quater) on the basis of which the UIF, as part of its powers, also on the basis of the provisions of Legislative Decree 231/2007, ascertains and alleges violations of Article 13.
[117] See Section 6.3.

8. COOPERATION WITH OTHER AUTHORITIES

8.1. Cooperation with the judicial authorities

International and European principles and rules call for broad cooperation among the authorities responsible for preventing and combating money laundering and the financing of terrorism. National legislation offers a variety of channels and networks for exchanging information, providing opportunities to coordinate and synergize prevention and suppression measures. This has given rise to various forms of cooperation with investigative bodies and the judiciary, each acting within their jurisdiction and according to the role and methods assigned to them.

While the UIF continues to fulfil its reporting obligations pursuant to Article 331 of the Code of Criminal Procedure – concerning offences uncovered in the performance of its duties – it also provides, at the request of investigating magistrates, information gathered in the course of in-depth analyses and inspections for use in investigations into money laundering, self-laundering, predicate crimes and the financing of terrorism. Specific forms of cooperation exist between the UIF and the National Anti-Mafia and Anti-Terrorism Directorate.

In turn, the judiciary and the investigative bodies share information with the UIF. This exchange helps the Unit to work more effectively by adding to its knowledge of criminal typologies and practices.

In 2017, the UIF continued to work closely with the investigative bodies and judicial authorities, including on several investigations that came to the public's attention.

The judicial authorities made a total of 226 requests, to which the UIF sent 429 responses (including follow-ups containing additional information, partly acquired from foreign counterparts) and related financial analyses (see Table 8.1).

Table 8.1

Cooperation with the judicial authorities

	2013	2014	2015	2016	2017
Information requests from the judicial authorities	216	265	259	241	**226**
Responses	445	393	432	473	**429**

The UIF cooperated in investigations into suspected criminal organizations, including cross-border ones, corruption, fraud and money laundering. The Unit's contribution was also sought in connection with cases of extortion, usury, organized crime, unauthorized banking and financial activities, tax offences and combating the financing of terrorism.

Reports

The decriminalization of certain offences, including some money-laundering offences,[118] is reflected in the decrease in the number of reports made pursuant to Article 331 of the Code of Criminal Procedure. The number of informative reports made for investigative purposes increased with respect to 2016 (see Table 8.2).

Table 8.2

Reports to the judicial authorities

	2015	2016	2017
Reports per Art. 331 CCP	233	157	**115**
of which:			
submitted to judicial authorities	*5*	*2*	***3***
made in connection with technical reports sent to investigative bodies	*228*	*155*	***112***
Informative reports for investigative purposes	17	16	**26**

The UIF continued to offer its experience and technical expertise to public prosecutor's offices throughout 2017, with each body performing its assigned role.

The UIF again exchanged information with the National Anti-Mafia Directorate as part of a panel of experts that includes the Customs and Monopolies Agency.

Memorandum of understanding between the UIF and the public prosecutor's offices of Milan and Rome

It signed memorandums of understanding with the public prosecutors' offices of Milan (27 January) and Rome (9 May 2017). On 5 April 2018, it signed a similar memorandum with the Naples public prosecutor's office.

These memorandums set out a framework for cooperation between the public prosecutor's offices and the UIF, and fully implement the rules on information sharing with a view to preventing and combating financial crime, the financing of terrorism and money laundering; they endorse established best practices; they regulate the sharing of information of mutual interest; and they announce the creation of focus areas for joint analyses of facts and information. The memorandums regulate the use of documentation and the electronic exchange of data, and envisage the introduction of reciprocal training programmes.

Memorandum signed with the Anti-Mafia Directorate

Memorandums[119] were also signed with the Anti-Mafia Directorate to regulate the forms of cooperation envisaged by the new anti-money laundering legislation. They extend the in-depth examination of situations brought to light by cross-referencing the respective databases.

SAFE

The new IT system to manage information sharing with the judicial authorities and foreign FIUs (SAFE) was introduced on 20 November 2017. The procedure digitalizes the entire process of acquiring and handling requests and information received using new IT channels and creating 'electronic folders' to replace the previous paper ones. Access to the portal provides new functions for dematerializing information

[118] Law 8/2016.
[119] See Section 1.3.2.

exchanges and processing cooperation requests or acquisition decrees addressed to the UIF. The procedure improves security and further protects confidential information.

The platform can be accessed after activating the Carta Nazionale dei Servizi (National Services Card) and sending a registration request to the UIF's certified e-mail address. Magistrates and investigative bodies can use a specific form to provide the information required in order to speed up searches in the UIF's database.

The UIF takes part in training programmes for new magistrates run by the Scuola Superiore della Magistratura, which offer the opportunity to illustrate the activity of the UIF and enhance reciprocal cooperation.

Thus, both sides continued to participate in each other's in-house training seminars with a view to increasing reciprocal knowledge of the tasks and tools involved in preventing and repressing financial crime. Closer contacts among the various parties and shared knowledge of available methods and information can help to ensure the effectiveness of any measures taken by the authorities responsible for preventing and combating money laundering and the financing of terrorism.

8.2. Cooperation with the Ministry of Economy and Finance and the Financial Security Committee and other forms of collaboration

The UIF works with the Ministry of Economy and Finance, assisting in drawing up prevention policies, drafting regulations and liaising with international organizations as regards sanctions. The UIF participates in the working group set up within the Ministry to examine jointly any complex queries raised by operators and to solve questions of interpretation regarding anti-money laundering legislation.

The UIF takes part in the work of the Financial Security Committee set up within the Ministry with a role of analysis and coordination to prevent the financial and economic system being used for money laundering or the financing of terrorism. All the authorities involved in this field sit on the Committee, which serves as a focal point for developing strategies to deal with known threats, including those that have emerged from the national assessment of money laundering and financing of terrorism risks. The Committee is in charge of adopting international sanctions and liaising with all the agencies and entities operating in the sector.

The Committee is assisted by a network of experts designated by the various member organizations, including the UIF. The network has a role of analysis and coordination; it also prepares summaries of issues on the agenda for meetings of the Committee, puts together supporting documentation on matters requiring approval, and studies topics brought to the attention of the Committee.

The FSC[120] is tasked with developing prevention strategies and conducting risk analysis at national level. The UIF is a member of the working group set up within the Committee for this purpose, charged with updating the NRA (National Risk Assessment) drawn up in 2014. A further working group on money-laundering and

[120] Cooperation with the Ministry and within the FSC concerned several profiles and subjects described in other parts of this report.

terrorism-financing statistics has been set up within the FSC to examine the data available to the system and improve their comparability where possible. This is part of the action plan approved by the FSC and designed to remedy the shortcomings that came to light in the course of Italy's Mutual Evaluation.

The UIF contributes to both working groups, providing analyses and statistics relating to its institutional activity and working alongside the Bank of Italy's supervisory directorates to develop risk indicators for evaluating the vulnerability of financial intermediaries.

8.2.1. List of 'designated' persons and measures to freeze funds

The UIF monitors the implementation of asset freezing measures;[121] these targeted financial sanctions have been established against the financing of terrorism and the activities of countries that threaten international peace and security.

The UIF therefore also collects information and financial data on funds and financial resources subject to freezing and helps to distribute and update the lists of designated persons.

The UIF's competencies with regard to international financial sanctions were recently confirmed in the new anti-money laundering legislation, which also allows the Ministry to adopt, on a proposal of the FSC, national measures to freeze funds in addition to those introduced by the EU.[122]

In 2016 the UIF received 6 notifications of asset freezes relating to persons or entities on the lists of those subject to such sanctions. Most of the cases related to updates of transactions on accounts held by designated Syrian banks that were specifically authorized by the FSC under the conditions provided for by EU law.

Data on the freezing of funds and financial resources were basically unchanged, except for the closure of some accounts following the debiting of expenses and fees and the de-listing of a number of persons, established by competent Authorities when elements collected against them in the course of investigations were not confirmed (see Table 8.3).

[121] Article 10.1, Legislative Decree 109/2007.
[122] See Article 4-*bis*, Legislative Decree 109/2007.

Table 8.3

Measures to freeze funds at 31/12/2017

	Accounts and transactions	Persons	Amounts frozen		
			EUR	USD	CHF
ISIL and Al-Qaeda	32	26	39,268	114	50
Iran	17	4	1,086,120	158,453	37,593
Libya	4	3	125,334	132,357	-
Syria	28	5	18,564,736	240,825	149,872
Ukraine/Russia	4	1	16,139	-	-
TOTAL	**85**	**39**	**19,831,597**	**531,749**	**187,516**

With regard to the fight against financing the proliferation of weapons of mass destruction, the European Union, in compliance with several resolutions passed by the UN Security Council, took further measures to tighten the financial sanctions against North Korea, the last of which was the adoption of Regulation (EU) No. 1509/2017 of 30 August 2017.

This Regulation introduces specific prohibitions on exports and imports and stringent restrictions on the provision of financial services (including a system of authorizations for money transfers above a given threshold), as well as a requirement to freeze the funds and financial resources of persons deemed responsible for the proliferation of weapons of mass destruction. Further restrictions on relations with the North Korean government include a prohibition on making real property available for use (except as relates to the conduct of diplomatic or consular missions) and the obligation to close bank accounts held by diplomatic or consular missions and their representatives (although a single account in the country may be allowed with prior authorization, in the case of Italy, of the FSC). Additional measures adopted by the EU include the obligation for financial intermediaries to report to their home FIU any suspicious transaction that could contribute to weapons of mass destruction-related programmes or activities.[123]

As part of its participation in the work of the FSC, the UIF performed assessments regarding compliance with asset freezing obligations, in particular examining requests made by UN panels of experts charged with verifying compliance with the contents of the Security Council's resolutions relating to the various sanctions in force.

8.3. Cooperation with supervisory authorities and other institutions

The legislation promotes cooperation between the various competent authorities and institutions at national level by providing that, notwithstanding official secrecy, the Ministry, the supervisory authorities, the UIF, the Finance Police, the Anti-Mafia Investigation Department (DIA) and the government agencies and entities concerned shall work together to identify circumstances that may point to facts and situations,

[123] See Article 23 of the Regulation.

prior knowledge of which can be used to prevent the financial and economic system from being used for money laundering or the financing of terrorism.

Exchanges of information with the Bank of Italy

The exchange of information between the UIF and the Bank of Italy's supervisory directorates continued to be vigorous and constructive. The directorates disclosed to the UIF reports of possible failures in active cooperation on the part of obliged entitites, discovered mainly in the course of inspections. The reports were investigated by the UIF and, in some cases, resulted in the initiation of administrative proceedings to impose sanctions for failure to report suspicious transactions.[124]

The UIF, in turn, sent reports to the supervisory directorates on dysfunctions at some financial intermediaries relating to their organizational structure, customer due diligence and recording of data in the single electronic archive (AUI).[125]

… with CONSOB

There was continued cooperation with Consob. The exchange of information involved notification to the UIF of failures to submit STRs uncovered in the course of supervisory inspections and analyses of market abuse. The UIF sent information to Consob relating primarily to anomalous transactions by financial consultants or auditing companies.

… and with IVASS

In 2017 the main purpose of information exchanges with IVASS was to check the absence of links between events relating to the governance of insurance companies and money-laundering or terrorism-financing activity.

The requests for information sent by IVASS often originated with its foreign counterparts. Given the confidentiality requirements applicable to shared data, the UIF transmitted to the FIUs of the countries concerned the data contained in its archives for use in money-laundering analysis profiles, providing its consent to inform local insurance supervisory authorities, in accordance with the restrictions imposed by domestic and international law. IVASS was notified of the procedures for cooperating with the foreign authorities concerned.

On 5 June 2017, IVASS asked life insurance companies to make a preliminary assessment of the risk of money laundering and terrorism financing for the year 2016, which will provide a basis for subsequent periodic reports.

Ministry of Economic Development and Customs and Monopolies

Based on the analyses carried out by the UIF on trust companies and gaming operators, information was shared with the relevant offices of the Ministry of Economic Development and the Customs Agency.

Consolidated Law on Immigration

A recent amendment to the Consolidated Law on Immigration[126] has introduced a new type of visa for foreigners wishing to make investments or charitable donations in Italy for large amounts. Such visas will only be granted after compliance with the related requirements has been verified, according to the procedure established by the decree of

[124] Cooperation with the supervisory directorates regarding the issue of sanctions has changed in the light of the new system introduced with Legislative Decree 231/2007, as amended by Legislative Decree 90/2017, which assigns the directorates new powers to impose sanctions for failure to report suspicious transactions on the part of supervised entities (see Section 1.3.1).

[125] The new anti-money laundering legislation repeals the provisions making it compulsory to enter data in the single electronic archive (AUI) and requires that data be preserved in order to comply with anti-money laundering requirements (see Articles 31 and 32 of the new Legislative Decree 231/2007).

[126] Article 26-bis of Legislative Decree 286/1998 introduced by Article 1.148 of Law 232/2016.

21 July 2017 issued by the Ministry of Economic Development, in agreement with the Ministry of Foreign Affairs and International Cooperation and the Ministry of the Interior.

Under Article 3 of the decree, the Investor Visa for Italy Committee will be the competent authority mandated to assess whether applications comply with the legal requirements. The Committee is chaired by the Ministry's Director General for Industrial Policy, Competition and Small and Medium Enterprises and consists of representatives of seven institutions, including the UIF. The UIF's role is to report on any records existing in the name of the visa applicant and to advise whether the country of origin of the funds contributed by the applicant appears on the list of 'third countries at high risk of strategic shortcomings'.

Ministry of Justice

In 2017 the UIF continued to act as advisor to the Ministry of Justice, submitting opinions on the codes of conduct drawn up by representative associations for the purpose of preventing the commission of offences.[127]

Anti-corruption coordinating committee

The UIF is a permanent member of the working group for the coordination of international action to combat corruption, which was set up in 2016 within the Directorate General for Globalization and Global Issues of the Ministry of Foreign Affairs. The working group has created a network to develop synergies and exchange information on Italian best practices and also ensures the alignment of Italy's position in the various international forums where anti-corruption strategies are discussed.

[127] Article 25-*octies* of Legislative Decree 231/2001.

9. INTERNATIONAL COOPERATION

9.1. Exchange of information with foreign FIUs

Within the international anti-money laundering system, the FIUs are given centralized responsibility for the tasks connected with receiving and analysing suspicious transaction reports and the related exchange of information with their foreign counterparties. The latter function is essential for the analysis of financial flows that increasingly go beyond national borders, and are therefore of interest to several jurisdictions.

Cooperation between FIUs is governed by the global standards of the FATF and the Egmont Group and by European rules. The standards require FIUs to provide, either spontaneously or on request, and in a timely, constructive and effective manner, the utmost cooperation at international level in the field of money laundering, associated predicate offences, and the financing of terrorism. The FIUs' capacity to exchange information is autonomous and direct, with no need for international treaties between governments. Memoranda of Understanding are negotiated and signed whenever they are required for cooperation by another FIU's national law.

In accordance with the principle of 'multidisciplinarity', for the purposes of domestic analysis and reciprocal exchanges the FIUs must have 'financial, investigative and administrative' information. In addition, FIUs must provide the information requested, exercising the same powers available to them for domestic analysis.

The exchange of information between FIUs takes place using rapid and secure electronic communication systems. At international level, the Egmont Group manages and updates the Egmont Secure Web, an encrypted platform for the exchange of information between FIUs.

At EU level, a decentralized communications infrastructure called FIU.NET is used, which permits a structured, bilateral or multilateral exchange of information and at the same time offers standardization, immediacy and secure data exchange.

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

Given the international nature of the most significant suspicious phenomena, the information acquired by foreign FIUs is particularly important for reconstructing the origin or use of funds or financial activities carried out abroad by persons under investigation in Italy. Exchanges of information are also essential for detecting the interpositioning of third parties in the ownership of assets and identifying the beneficial ownership of entities and companies; in these cases, cooperation between FIUs is vital for reconstructing schemes based on setting up companies or transactions in various countries in order to exploit loopholes in the safeguards and controls.

The need for efficiency and for sharing large volumes of data has fostered the growth of new forms of cooperation based on automatic and structured multilateral and information exchanges.

Overall, the UIF exchanged information with 101 FIUs (an increase compared with the previous year's figure of 87), of which 27 from EU countries.

As part of its remit to analyse STRs, the UIF sends requests for information to foreign FIUs whenever subjective or objective links with other countries come to light. The requests usually seek to reconstruct the origin or use of funds transferred to or from other jurisdictions, to identify movable or immovable assets abroad, and to clarify the beneficial ownership of companies or entities established in other countries.

The UIF's cooperation with its foreign counterparts is of fundamental importance for the analysis of STRs and for detecting cases of economic crime and money laundering on a transnational scale. The exchange of information enables the UIF to provide the investigative bodies and the judicial authority with additional information to support their criminal investigations and proceedings. The information thus obtained proves very useful for work on investigations and criminal proceedings and the use of letters rogatory. Experience has shown that, thanks to this cooperation network with its foreign counterparts, the UIF is able to intercept and quickly recover any cash flows channelled towards other jurisdictions.

Requests sent to foreign FIUs

In 2017 the UIF sent out 763 requests for information, confirming the growing trend of recourse to international cooperation in recent years (see Table 9.1). The increase was particularly marked (+74 per cent) for requests made to support the analysis of suspicious transactions, in order to build on links detected abroad.

Table 9.1

Requests sent to FIUs in other countries

	2013	2014	2015	2016	2017
Information required for the judicial authority	124	146	217	204	**172**
Information required for internal analysis	56	242	323	340	**591**
Total	180	388	540	544	**763**

The increase in exchanges also stems from the growing use of the 'Ma3tch' function provided by FIU.NET for the anonymous matching of entire databases, thanks to which it is possible to identify recurring names in the archives of participating FIUs and links with other countries that do not emerge from the analysis of a case. The Unit has systematically applied Ma3tch to large datasets relating to reported subjects: over thirty information exchanges have been activated on the basis of identified matches, especially in relation to activities suspected of being connected with the financing of terrorism.

Developing Ma3tch and how to use it in a uniform way is central to the work of a dedicated group set up by the European FIUs' Platform, in which the UIF participates.

This development is also necessary in order to complete the automatic exchange system for cross-border reporting, of which Ma3tch is an essential part. The group's objectives are to encourage its systematic use by all European FIUs, to broaden the types of data made available for matching and to have them updated more frequently.

The greater use of Ma3tch has contributed, in line with trends in recent years, to the decrease in 'known/unknown' requests (31 in 2017), whose sole objective is to determine the existence of reports on given persons or entities in other countries.

Requests received from foreign FIUs

In 2017 the UIF received a total of 2,246 requests and spontaneous communications from foreign FIUs. The consolidation of this figure, following the peak of 3,314 reached the previous year, confirms the high number of international exchanges involving the UIF (see Table 9.2).

Table 9.2

Requests/spontaneous communications received and responses provided

	2013	2014	2015	2016	2017
Egmont network	519	486	1,078	1,259	668
Requests/spontaneous communications	*519*	*486*	*695*	*723*	*504*
Exchanges re ISIL			*383*	*536*	*164*
FIU.NET	274	453	1,075	2,055	1,578
Requests/spontaneous communications	*274*	*453*	*518*	*580*	*524*
Cross-border report			*557*	*1,475*	*1,054*
Total	**793**	**939**	**2,153**	**3,314**	**2,246**
Responses provided *	**1,066**	**1,144**	**1,223**	**1,568**	**1,232**
Communications to investigative bodies	**557**	**713**	**868**	**1,430**	**2,031**

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

The fall in the number of requests and spontaneous communications, which is greater for exchanges with non-European FIUs (Egmont channel), is in part attributable to the change in practices towards exchanges that focus more on the existence of actual links emerging from better preventive analysis. At European level, the decrease in the number of requests through FIU.NET should be seen as the result of the greater use of Ma3tch which prevents 'useless' requests by pre-identifying existing links.

Multilateral exchanges on ISIL

The exchanges on ISIL deal with activities traceable to financial support for it provided through international remittance networks. These activities are detected through objective elements, irrespective of any reference to actual suspicion, and shared with FIUs that might be interested even if there are no specific territorial links. This has

made it possible to accumulate a significant amount of information useful to the FIUs for developing preventive intelligence on how ISIL is financed.[128]

The decrease in the volumes of these multilateral exchanges compared with the previous year reflects the developments in the 'ISIL Project', within the Egmont Group, which is now in its third phase: the focus of financial intelligence has shifted from the detection of complex financial networks responsible for financially supporting ISIL as a 'state' organization to the detection of more limited financial support for fighters returning from areas of conflict and settling back in their country of origin, and for recruitment and propaganda activities.

Automatic exchanges of reports

Alongside the exchanges of requests and spontaneous communications between FIUs, and in order to implement some cooperation practices already under way, the Fourth AML/CFT Directive introduced the obligation to automatically exchange STRs displaying cross-border characteristics: the FIUs must promptly submit to their European counterparties any request 'which concerns another Member State'.[129] This mechanism aims to mitigate the potential distortions caused by the territoriality criterion, which requires that suspicious transactions be reported to the FIU of the country in which the reporting entity is based, even if the transactions are carried out abroad under the freedom to provide services.

The number of cross-border reports received by the UIF, albeit lower than in 2016, is double the figure for 2015, when automatic exchanges were first launched. This figure should be interpreted in light of the technical difficulties encountered in forwarding the reports by the FIUs responsible for most of them.

The system for the automatic exchange of cross-border reports

Although the FIU.NET system has been supplemented with functions dedicated to automatic exchanges of cross-border reports, frequent service interruptions have so far prevented it from working efficiently.

In addition, the European FIUs are still working on the necessary technical and procedural adaptations, especially for the instruments for importing and exporting information into or from their systems. Not many FIUs have activated systematic exchanges of cross-border reports and some of those who have are encountering problems in sending large volumes of information, while others have gone back to manual procedures.

The effectiveness and the volumes of cross-border report exchanges suffer from a lack of shared criteria and of uniform technical instruments for sending large amounts of information automatically. In 2017, work continued on defining uniform criteria for identifying and exchanging cross-border reports. The FIUs Platform, as part of a project in which the UIF participates, approved an initial series of criteria that identify the relevant links for automatic transmission, defining the information useful for analysis and in order to avoid excessive reporting flows.

[128] On this point see Annual Report of the UIF on activities carried out in 2016, Chapter 7.
[129] Article 53(1) of the Fourth AML/CFT Directive.

According to these preliminary criteria, cross-border reports include, first of all, those made by entities operating in member states under the freedom to provide services. The cross-border nature of reports is also determined on the basis of subjective elements (residence or the existence of investigations in other countries) and objective elements (foreign country of origin or destination of financial flows or the country in which financial accounts or relationships are maintained). These criteria also focus on the involvement in illicit activities carried out in another country, or the importance of the case for other countries based both on elements of risk found in specialized databases and on discretionary assessments.

Responses provided

In response to requests or information received, the UIF sent 1,232 responses to foreign FIUs. This figure includes responses to requests for cooperation and feedback on the use of what is received in the form of spontaneous communications which did not ask for specific cooperation. The UIF also provided responses on the quality of the assistance received, at the request of some counterparties.

The growth in the volume of information from international exchanges and sent by the UIF to national investigative authorities is particularly significant. The figure in question (+41 per cent) also reflects the expansion of these types of dissemination which are addressed not only to the Special Foreign Exchange Unit of the Finance Police and the Anti-Mafia Investigation Department but also to the authorities competent to investigate particular criminal offences, in compliance with international principles.

Several communications relating to the financing of terrorism were sent to the Special Operations Group of the Carabinieri. Other communications, traceable to the trade in child pornography material, were shared with the State Police's National Centre for Combating Child Pornography. All the communications from abroad were sent to the investigative authorities in compliance with the prior consent of the counterparties involved, with special precautions adopted to protect confidentiality and to limit their use.

'Diagonal' exchanges

Alongside the direct exchanges between FIUs for analysing cases of money laundering or financing of terrorism, forms of 'diagonal' cooperation are being developed that involve other foreign authorities or that aim to use the FIUs' information for additional purposes.

The Unit continued to cooperate, via the local FIUs, with foreign supervisory authorities in order to verify, in connection with enquiries into the governance of supervised companies, any links with money laundering or financing of terrorism activities. Through the FIUs, the UIF also provided cooperation to investigative authorities in foreign countries working on investigations of particularly complex cases. Information exchanges have been set up with foreign FIUs as part of vetting programmes in relation to specific risks of corruption and financial crimes, in order to assess the appropriateness or lawfulness of public figures' assets in the countries involved.

The UIF takes part in these types of diagonal cooperation in compliance with the provisions of national legislation and with international and European standards. Specifically, this implies the application of tight constraints on the use and sharing of the information provided. In addition, in exchanges of this kind, the UIF always directly and immediately involves the FIUs in the countries concerned.

SAFE

The entry into force of the IT system for managing exchanges with the judicial authorities and the foreign FIUs (SAFE) makes it possible to manage on an integrated basis the exchanges with foreign counterparties safely and so as to protect confidentiality.

9.2. Cooperation between FIUs

There has been some improvement in the quality of the cooperation received from foreign FIUs, despite significant and persistent problems. The requests and communications received from some counterparties, especially European ones, include information of greater depth and breadth as regards the description of the case and the grounds for suspicion. There has been similar progress in the response given to requests for information; the capacity to acquire and exchange financial information, often obtained specifically from obliged entities, seems to have increased.

These improvements, to be verified over time, can be driven by the legislative reforms carried out in European countries for transposing the Fourth AML Directive, which requires an increase in the capacity of the FIUs to access information for their analyses and to exercise the information-gathering powers available, also to provide cooperation to foreign counterparties.

There are still significant obstacles that limit the effectiveness of information exchanges. These are linked in particular to the inadequate information-gathering powers of various FIUs, to the application of limiting conditions (e.g. ongoing criminal investigations or proceedings) or to constraints on the use of the information for subsequent investigations. These obstacles are the result of several factors, the most frequent examples being the nature of each FIU, the absence of a clear dividing line between financial analysis and investigations (e.g. Law Enforcement type FIUs) and financial or professional secrecy obligations.

At European level, the initiatives of the EU FIUs Platform designed to boost the sharing of methodologies for analysis and for carrying out joint work on important cross-border matters can foster operational integration and develop common practices and approaches to help overcome the still considerable differences between FIUs.

9.3. Changes to the FIU.NET

Over the last few years, FIU.NET, operational since 2002, has undergone a rapid obsolescence while transitioning to Europol, due above all to the gradual increase in the volumes of data exchanged and to the variety of exchange types and formats (e.g. alongside traditional ones, there are now particularly intense exchanges of cross-border

reports). Europol has pointed out the need for a radical restructuring of the network, drawing up an initial 'Roadmap' for this purpose, which received several critical comments from the FIUs.

The project provided for a centralized configuration for the network with Europol storing the information exchanged between FIUs (without this agency being able to access it, except in cases where the FIUs give their explicit consent). The system was meant to stay the same, however, as far as the Ma3tch functions are concerned.

The FIUs, both on the EU FIUs Platform and in the Advisory Group set up within it to take part in the management and governance of FIU.NET, have highlighted the need for more information and analysis of the characteristics of the interventions and the final configuration, as well as for adequate guarantees for maintaining full control over information. The opportunity to set out and analyse alternative solutions for the future configuration of the system was requested, based on decentralized systems for the exchange and the conservation of information.

The UIF, in particular, highlighted the need for a review of the system which must comply with some essential conditions: maintaining a focus on cooperation between FIUs; FIUs maintaining ownership and full control of the data they exchange; the FIUs' involvement in planning, development and governance; and maintaining alternative options, not necessarily centralized ones.

The critical comments made by the UIF broadly inspired the standpoints of the EU FIUs Platform, which reserved for itself all the assessments of the characteristics and practical functions of the new system, and of the Advisory Group, which summarized them in an 'Opinion' inviting Europol to redesign the 'Roadmap'.

The analyses, still under way, also recognize the regulatory and operational constraints involved in the possibility of a centralized conservation of the data involved in exchanges, with particular reference to the implications for data protection, security and the responsibility inherent in a centralized configuration, identifying technical solutions for data encryption, setting time limits for storing information in Europol's archives and guaranteeing the maintenance of adequate time series on the exchanges made.

9.4. The EU FIUs Platform

Following the adoption of the final report on the Mapping Exercise the UIF, in agreement with the European Commission, drew up a document summarizing the main proposals, with the relative development policies, according to the interlocutors concerned: European institutions, national regulators and FIUs. The projects and activities to be carried out on the Platform for implementing the Report are outlined, and a broad range of matters of interest for the FIUs are identified: 'nature and organization'; 'autonomy, independence and accountability'; functions and powers', 'information received and that can be acquired'; and 'international cooperation'.

To make identifying the projects and activities to be undertaken more granular and to make it easier to assess the work requested and the priorities, 84 problem areas have been identified together with possible steps to be taken.

The document prepared by the UIF provided the basis for the discussion of the new Platform Work Plan approved in 2017: it includes all the areas for intervention identified in the Mapping Exercise, outlining specific projects or initiatives for each one.

The Work Plan is heavily oriented towards projects that are of practical use for the FIUs' work, especially in recognizing the content of STRs, identifying a minimum range of information that must be available for analysis, and defining how to make wider use of the information exchanged. Direct involvement at operational level is provided for, with the aim of making a forum available to the FIUs for increasing cooperation also through greater integration, and especially by setting up joint analysis initiatives, as envisaged by the Fourth Directive.

The projects for developing the Mapping Exercise received positive feedback from the FIUs. The UIF, in keeping with its strategic role in the mapping exercise, is directly involved in five projects and is coordinator for two of them.[130]

Because of its characteristics and the work plan being developed, the Platform is the obvious place for creating advanced forms of integration and coordination between the European FIUs. It can provide the most suitable framework in which, as envisaged in the Fifth Directive, the Commission will be able to draw up proposals for a 'coordination and support mechanism' to improve the analyses and the cooperation between the FIUs.

9.5. Relations with foreign counterparties and technical assistance

Protocol with the Chinese FIU

On 20 June 2017, the Unit signed a cooperation Protocol, drawn up in compliance with FATF and Egmont Group standards, for information exchanges with the FIU of the People's Republic of China (China's Anti-Money Laundering Monitoring and Analysis Centre – CAMLMAC), established at the local Central Bank.[131]

The signing of the Protocol occurred at the end of a series of analyses begun in 2014 to verify the characteristics of the two Units, identify the information sources available to them and ascertain the capacity and conditions for exchanges. The text of this Protocol takes account of the existing differences and focuses on the essential aspects of cooperation.

This agreement is necessary for the Chinese FIU to carry out bilateral cooperation. It makes it possible to launch information exchanges potentially useful for reconstructing and analysing the complex operational schemes that characterize financial flows between Italy and China.

Technical assistance

In 2017 the UIF continued its efforts in the field of international technical assistance in its sphere of competence through bilateral initiatives and participation in multilateral projects.

---

130 In a case together with the Dutch FIU.

131 The UIF currently has a memorandum of understanding with the foreign counterparties of the following 25 countries: Australia, Belgium, Bulgaria, Canada, China, Croatia, the Czech Republic, France, Japan, Greece, Guatemala, Guernsey, the Holy See, Indonesia, Latvia, Monaco, Panama, Poland, Romania, Russia, Singapore, Slovenia, Spain, Ukraine and the United States.

The Unit received numerous requests for technical assistance. Many of these arose from the positive outcome of the Mutual Evaluation Report on Italy which underlined the quality, sophisticated nature and effectiveness of the activities and tools available to the UIF, as well as the innovations in the procedures and practices for domestic analysis and international cooperation.

The productive dialogue with the Iranian FIU continued, which had begun the previous year following the weakening of the international financial sanction regime against Iran.

During specific bilateral meetings, some topics were explored in connection with, among other things, organizational aspects (resources available, independence requirements, operational procedures), the range of information available for analysis, the management and analysis of STRs, and the development of indicators to detect suspicious cases and rating systems to support the analyses. These meetings were also an opportunity to set up and develop bilateral cooperation between the UIF and the Iranian FIU by exchanging information to deal with specific cases.

In 2017 too, the Unit made a contribution to the training scheme sponsored by the Ministry of Foreign Affairs and International Cooperation on the analysis of and investigation techniques for financial flows, hosting a delegation of officials and police officers from countries of the Caribbean Community (CARICOM) and from Cuba. The training carried out by the UIF focused on the tools and methodologies for analysing transactions suspected of money laundering and financing of terrorism and on international cooperation.

The Unit also helped to organize a study visit to the Bank of Italy by representatives from the People's Bank of China. One session looked at the UIF's role in preventing and combating money laundering in the financial sector, and the operational tools and the practices for reporting and analysing suspicious transactions and for international cooperation were presented.[132]

In addition, the UIF continues to be part of the technical assistance carried out by the Egmont Group's working groups (especially the Training and Technical Assistance Working Group). These schemes are generally addressed to FIUs that are being set up or that need training and capacity building programmes to develop their analytical skills, operational procedures and information tools, as well as international cooperation. This leading role, taken on by the Egmont Group in sensitive geographical areas, has fostered the creation of new FIUs and their membership of the organization itself.

9.6. Participation in the FATF

Given the importance of international cooperation for combating money laundering and terrorism effectively, several governmental and technical bodies have been set up over time, whose scope varies from regional to global. The activity of these bodies is especially intense in relation to the different types of risks that emerge at

[132] The UIF took part in a similar programme in 2015.

global level and to the need to adapt and harmonize the measures to prevent and combat these phenomena.

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

The FATF's activities

In 2017, the UIF regularly participated in the work of the FATF within the Italian delegation coordinated by the MEF, and was a member of various working groups. There was a particular focus on the fourth round of Mutual Evaluations of member countries: the UIF made its contribution to both the preparation phases, drawing up documents analysing specific risks and the quality of the cooperation received, preparing and discussing the reports, sending comments and proposals on priority themes, and through direct participation in the assessment of some countries.

Over the last two years, the UIF's experts have been directly involved in assessing Belgium, Canada, Austria and Switzerland and in the follow-ups on Spain and Belgium. Furthermore, in 2018 the UIF's experts are going to take part in the Mutual Evaluation by Moneyval of Malta (with an assessor) and of the Czech Republic (with a reviewer). In 2018, the follow-up assessment of Italy will begin, which will evaluate the progress made in the technical compliance with the new anti-money laundering legislation introduced with the transposition of the Fourth Directive.

Participating in assessment activities has produced positive results, highlighting in particular problems in the national legislations and practices relating to the characteristics and activities of the FIUs concerned and the relevant international cooperation.

The UIF took part in the analyses, launched by the FATF in close cooperation with the private sector, of the implications of new technology applied to the financial industry (FinTech), also as regards the development of support tools that are effective for compliance (RegTech).

FinTech

International anti-money laundering organizations are very interested in the IT innovations applied to finance (FinTech). The FATF has organized a great deal of fact-finding activity, in close cooperation with the private sector, as a precursor to the specific recognition of risks and to checking the adequacy of the current standards. This has also been useful for assessing initiatives and safeguards that make the best use of the benefits of IT innovation and enable the adequate prevention and detection of offences and anomalies attributable to money laundering and the financing of terrorism.

The FATF set up several meetings with the private sector in 2017. A 'Roundtable on FinTech and Regtech' was held in the margins of the Plenary session in February; one session of the 'Private Sector Consultative Forum' in March was dedicated to a 'Dialogue on FinTech and RegTech'; and in addition, two meetings of a specific 'FinTech and RegTech Forum' were organized in May and October. In 2018, roundtables were set up within the working groups to draw up some new standards and guidelines.

The firms operating in the FinTech and RegTech sectors are mainly start-ups specializing in the management of online platforms and apps that provide financial services for transfer, payment or direct intermediation between private individuals. The activities carried out are often based on big data management and on the use of blockchain technology for using cryptocurrencies. The most advanced services include those relating to P2P money transfers, remittance services, and private fundraising, such as crowdfunding, crowdlending and crowdinvesting.

The new technology makes it possible to provide innovative services or services with new features, not always uniquely ascribable to the regulations currently in force; it also enables particularly lean and efficient organizational solutions to be found for their supply and distribution. Fostering innovation has beneficial effects on the costs for firms and for customers; the competition that is created, especially for traditional operators, may redefine the provision of financial services and influence customers' behaviour and the business model for intermediaries.

At the same time, carrying out innovation makes it necessary to verify the requirements envisaged by the current legislation, their adequacy and the effectiveness of the controls. Discussions with the private sector highlighted the benefit that using innovative technical tools has on the effectiveness of anti-money laundering compliance. This benefit is particularly pronounced in the handling of large amounts of information, and is often indispensable for appropriate risk management, customer monitoring and detecting suspicious transactions.

It was made clear how monitoring activities for identifying suspicions can be made more effective by using technology that integrates 'human' analysis. Machine learning and data mining tools make it easier to select information, identify links that are not apparent and predict probable behaviour and connected anomalies. Distributed Ledger Technology, which is the basis of the diffusion of virtual currencies, can also provide support for monitoring and assessment.

The analyses carried out by the FATF revealed the importance of financial innovation combined with the effective application of the anti-money laundering and counter-terrorism safeguards; the new risks have to be mitigated without hindering the progress of innovations. Updated rules and controls need to remain proportional to risk and neutral from a technological point of view. A level playing-field can be ensured by avoiding national gaps and international misalignments.

The UIF also took part in the analyses of the updated typologies of money laundering and financing of terrorism, giving the benefit of its experience and providing practical operational examples for reconstructing illegal activities carried out by misusing the beneficial ownership of entities and companies, of financial flows from human trafficking, and of the features of money laundering set out by 'Professional Money Laundering Networks', also at international level.

Forum of FIU Heads

The efforts to contribute to the work of the Forum of FATF Heads of FIU have continued this year too. The Forum identified, also with reference to the experience and results of the European Mapping Exercise, some areas for intervention where it seems appropriate for the FATF to draw up guidelines or standards to increase the

effectiveness of the FIUs' work and cooperation. In 2017, a document setting out the priority courses of action was approved.

The Forum is also continuing its efforts to foster partnerships between FIUs and the private sector, especially to support active cooperation for detecting and reporting cross-border suspicious transactions.

The FIUs' autonomy and independence

The organizational characteristics and the autonomous and independent status of the FIUs have a direct impact on their functions, powers, cooperation and the overall effectiveness of prevention.

Based on wide-ranging fact-finding activities, the Forum gives priority to analysing the requirements for autonomy and independence according to international standards. A specific document was dedicated to this topic, showing why these requirements are important, where they are relevant, and the problem areas needing intervention.

The document confirms that autonomy and independence are essential preconditions for the FIUs to work effectively to identify and analyse significant criminal phenomena and cases. Protection from any form of interference has to be ensured both at organization and governance level and for carrying out fundamental analysis, cooperation and dissemination.

At institutional level, autonomy assumes that a FIU is separated in organizational terms from the institution to which it belongs, it is provided with suitable human, financial and technical resources that can be used with discretion based on needs, and is able to make decisions that do not depend on an external authority. The guarantees necessary for this include the availability of an adequate and separate budget, the absence of hierarchical constraints on the management or staff of a FIU towards third parties, and the capacity to decide on the organizational aspects required for it to work effectively and to hire and allocate the necessary human resources.

With reference to functions and powers, independence is seen above all in the capacity of the FIUs to launch and orient their analyses based solely on technical considerations regarding the potential criminal importance of the facts. Analytical tasks and the relative powers must be kept absolutely separate from those of the investigative authorities and cannot be influenced or limited by the existence of investigations and criminal proceedings. This has to be matched by the availability of adequate information-gathering powers: access to information must be wide-ranging and direct, and cannot depend on third-party assessments or authorizations.

The document focuses on law enforcement agencies' information, making it clear that the FIUs must be able to request and obtain data from police forces and intelligence agencies, and should in turn share with them any available elements of interest.

Disseminating the intelligence processed and the results of the analyses has to be done independently too. The document underlines that the objective of effectively developing reporting and analyses presumes that a FIU is in any case able to decide

which authority or organization is going to receive communications, the content of the information and its format.

Autonomy and independence are also essential elements for sustaining international cooperation. The FIUs must be able to exchange information directly with their foreign counterparts, exercising their powers to that end; any memoranda of understanding must be drawn up and signed autonomously. Cooperation must be given without influence regarding any ongoing investigations (although taking the precautions necessary to avoid any damaging interference). Autonomy also guarantees that the information exchanged is used in compliance with the principle of the consent of the counterparty that provided it, ensuring its confidentiality as regards accessing or using it for further purposes (e.g. for investigations or criminal proceedings).

At the same time, the document underlines that autonomy and independence accentuate the responsibility of the FIUs regarding the other competent authorities, the political sphere and the general public. They must try and achieve a suitable balance between forms of fair cooperation with the other institutions and accountability in order to guarantee transparency in their work and awareness of their results.

The document prepared by the FATF's Forum of FIU Heads was approved in the Plenary session. As well as informing possible further initiatives for clarifying standards or guidelines, it also provides useful references for adapting organizational structures.

9.7. Participation in other international organizations

The Egmont Group

The UIF also contributes to the work of the Egmont Group in all its various bodies, and promotes its policies. A particularly important part of the Group's activities are the Support and Compliance procedures, launched when an insufficient rating is assigned in the Mutual Evaluations in relation to aspects of the FIUs of the countries concerned. This procedure specifically focuses on analysing the problems in international cooperation and aims to foster corrective measures, also through specific technical assistance schemes, and to apply sanctions. The UIF took part in the reviews of the Swiss and Austrian FIUs.

In 2018 the Group will set out the expansion of the Support and Compliance procedure (currently limited to 'technical compliance') to assess the effectiveness of the FIUs' work, with regard to analysis (Immediate Outcome 6 of the FATF Methodology) and international cooperation (Immediate Outcome 2).

The Egmont Group's work in further analysing the updated types and areas of risk remains focused on the financing of terrorism.

The analyses carried out as part of the ISIL Project are important for the development of antiterrorism intelligence activity by the FIUs and to increase the related forms of cooperation. The FIUs are currently involved in the third phase of the Project (financing returnees and the threat of lone wolves), and are working on identifying lines of action and possible new forms of reciprocal cooperation.

Other activities

The UIF is a member of the Italian delegation to Moneyval and follows its activities. It also has a scientific expert involved in the Conference of the Parties to the Warsaw Convention of 2005 on money laundering and the financing of terrorism.

10. ORGANIZATION AND RESOURCES

10.1. Organization

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

The Director is also assisted by the Advisory Committee for the Review of Irregularities. This is an internal collegiate body which is responsible for: analysing suspected irregularities uncovered by the UIF in order to initiate sanction procedures, forwarding reports to judicial and sectoral supervisory authorities and investigative bodies, and taking any other initiatives deemed necessary.

As required by law, the Unit is also assisted by a Committee of Experts, whose members include the Director of the UIF and four experts appointed for three years by decree of the Ministry of Economy and Finance after consultation with the Governor of the Bank of Italy. The Committee is a valuable forum for discussion that lends ongoing support to the UIF's activities and provides insights into the most pressing topics of the day.

In 2017 the Director's mandate was renewed for a further five years and four new members of the Committee of Experts were appointed.[133]

10.2. Performance indicators and strategic plan

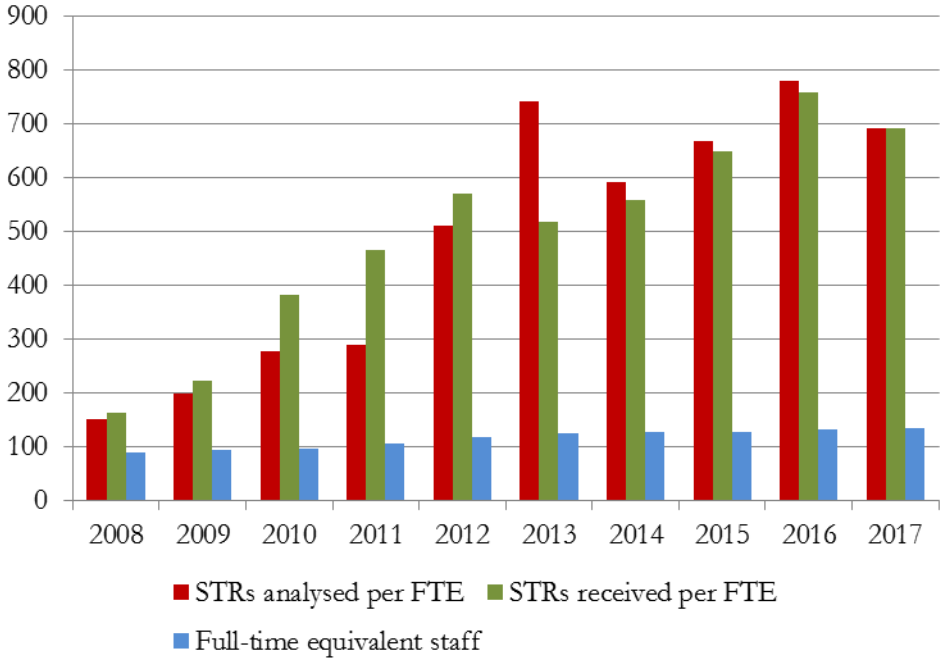
In 2017 the standard performance indicator, i.e. the ratio of the number of suspicious transaction reports (STRs) analysed per full-time equivalent (FTE) employee, came to 692. Though still slightly below what it was in 2016 (Figure 10.1), this was nonetheless a very high figure. The downward variation reflects the reduction in the number of reports received and the full clearance of the backlog (at the end of the year, the number of reports still being processed amounted to around 4,500, corresponding to less than 60 per cent of monthly average inflows of STRs).

Moreover, the indicator tends to underestimate actual productivity levels, especially in periods when a number of activities that are not linked (either directly or indirectly) to the processing of STRs assume particular prominence. This effect was apparent in 2017 when the indicator failed to capture the intensive utilization of staff members to help draft the legislation for transposing the Fourth AML Directive and, subsequently, for implementing its provisions.

[133] Decree of 9 March 2017.

Figure 10.1

Ratio of STRs received and analysed to FTE staff



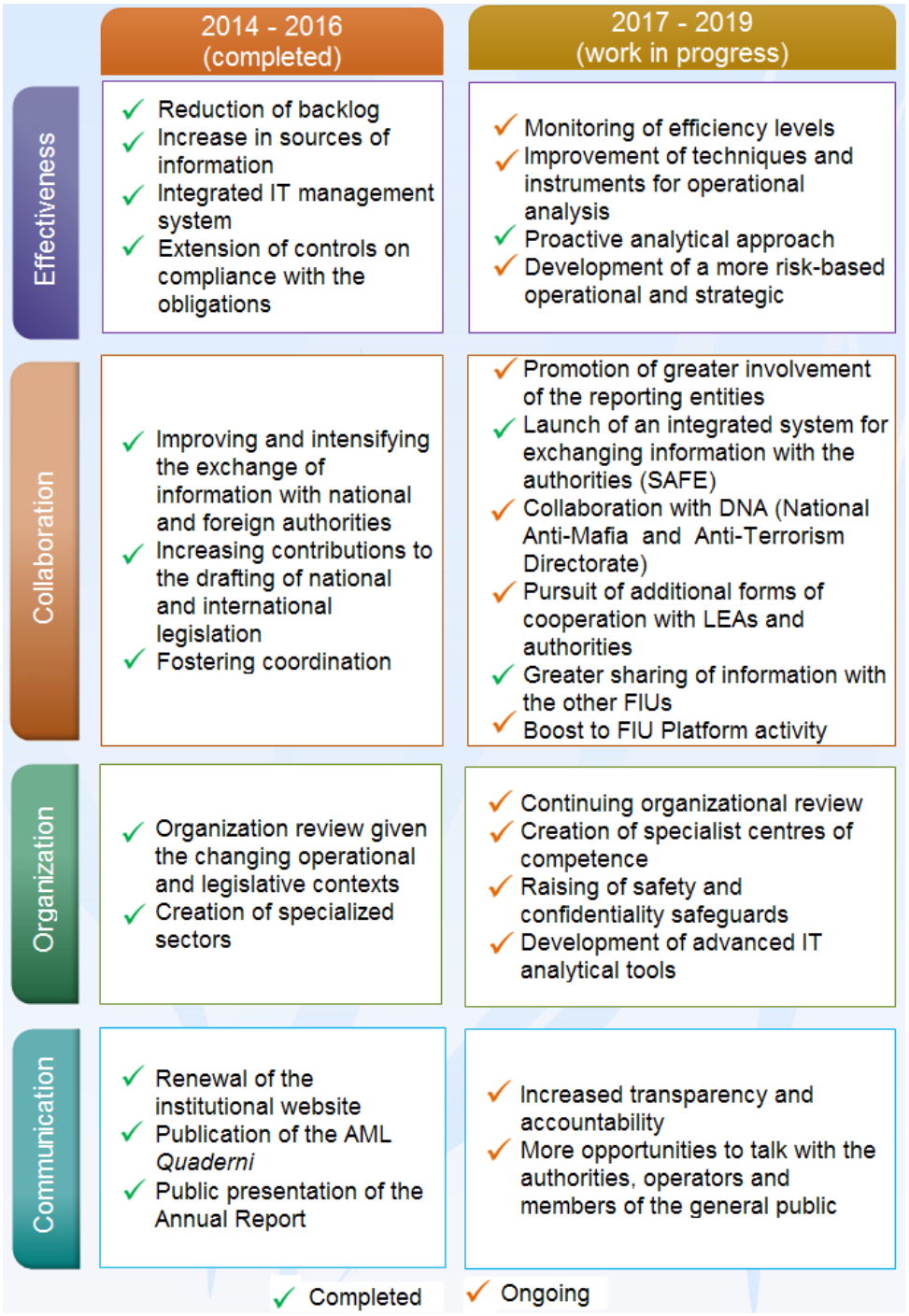
The definition of the strategic guidelines

The UIF draws up its strategic action plan every three years. The previous plan, covering the years 2014-16, achieved all of the set objectives; the 2017-20 plan contains new and ambitious goals.

Among other things, the Unit will continue to develop analytical methodologies and instruments, including IT tools, which will make it easier to process and select data from the mass of information it receives, favouring a more proactive and risk-based approach and greater analytical depth when it comes to specialist analyses. Considerable efforts have been devoted to improving information sharing and cooperation both with the reporting entities and with the other foreign authorities and FIUs, also thanks to the use of new communication tools. On the organizational front, the UIF has constantly adapted its processes to address the significant increase in its volume of activities and to further improve its monitoring and accountability procedures.

Figure 10.2

Overview of the UIF's previous and current three-year strategic plans



The strategic planning of the FIU is currently being updated to take account of the effects of implementing the 2017 legislative reform. This has entailed new operational tasks (such as those linked to threshold-based communications and the broadening of the platform of institutional interlocutors) and regulatory functions (for

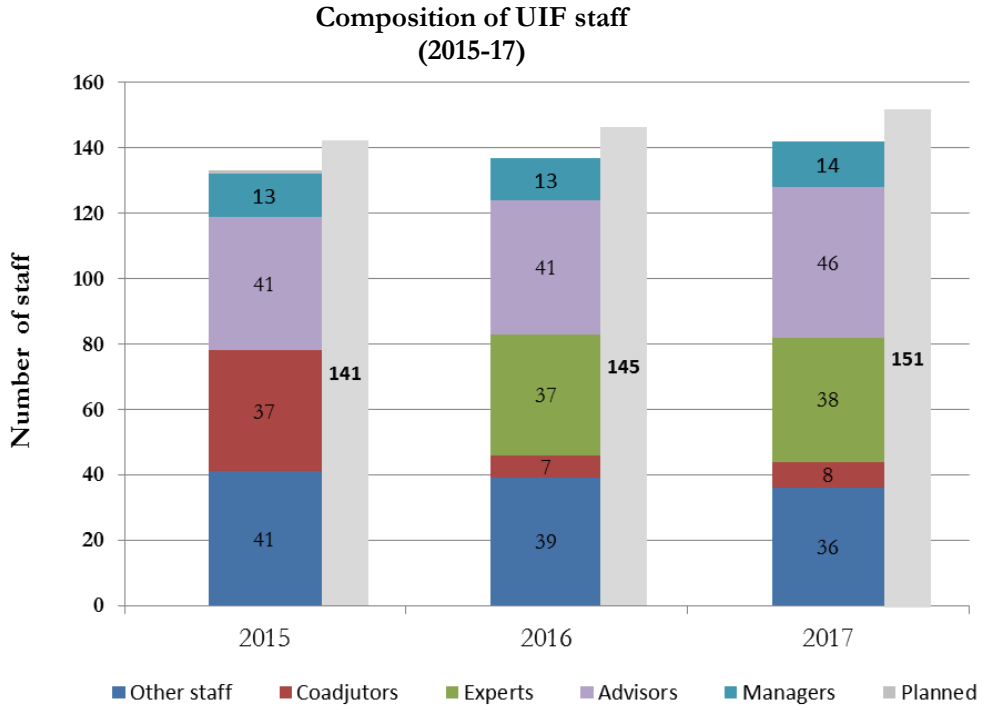
example, the Public Administration guidelines), which in turn have affected how the Unit is structured.

10.3. Human resources

In 2017 the number of UIF staff members increased from 137 to 142, as a result of the exit of 5 and the addition of 10 members, of which 4 new hires and 6 from other areas of the Bank of Italy selected via internal hiring processes (Figure 10.3).

The shortfall with respect to a projected staff corpus of 155 persons remains significant, though this is gradually being addressed. As at 31 December 87 members of staff were assigned to the Suspicious Transactions Directorate while 51 were assigned to the Analysis and Institutional Relations Directorate.

Figure 10.3



Maintaining highly-skilled staff calls for a commitment to ongoing and multidisciplinary training. In addition to organizing internal seminars and participating in conferences on measures to counter money laundering and the financing of terrorism, special attention was devoted to staff training in key areas for the Unit, such as combating corruption, IT developments in payment systems (often in relation to new instruments), the problems raised by crypto-assets and, more generally speaking the digital economy. The topic of Big Data, an especially important area for the development of the UIF's analytical systems and sectoral studies, was another important focus of staff training.

Intensive training was also supplied on a range of issues relevant to the financial system and controls, with contributions from various Directorates General of the Bank of Italy, ESCB initiatives and activities organized by other sectoral authorities.

10.4. IT resources

During 2017, work continued on the realization and implementation of IT systems designed to support the Unit's activities. Their development helps integrate individual sectors within the Unit into a cohesive whole, in order to increase synergies between the information available to the various areas of competence.

Special emphasis was accordingly placed on the development of work tools and communication systems to support national and international cooperation. The projects that have been completed or are nearing completion aimed to help make more widely available the Unit's body of information by automating and integrating the internal and external transmission of documents into internal processes.

Sharing information with JAs and FIUs (SAFE)

In the second half of 2017, the project for sharing information with foreign authorities and Units, SAFE for short, was completed.[134] The system uses electronic channels to acquire information from the judicial authorities, investigative bodies and other FIUs and has automated the entire process for handling requests. This has led to much more automation, significantly less manual work, a sharp decline in the use of paper-based materials and, ultimately, greater efficiency. The second phase of the project is currently under way and among other things will develop additional monitoring functions.

Data security and protection

Last year too, partly in relation to the release of SAFE, special attention was paid to IT security issues and the protection of sensitive data used to achieve institutional objectives. There is ongoing and increasingly intensive monitoring of IT systems and work processes with the objective of ensuring that the technical and organizational safeguards in place meet security standards. These safeguards must be constantly adapted to take account of external developments such as new legislation, emerging threats and innovative technologies. To verify this, in 2017 the Unit requested an internal audit by the Bank of Italy's Internal Audit Directorate.

A number of steps are currently being taken to strengthen internal security and the traceability of access on the part of the Unit's management.

Threshold-based communications

In 2017, several additional projects were launched to implement the new provisions of the AML Legislative Decree. Starting last autumn, the Unit launched a number of activities to complete the IT systems for collecting and using threshold-based communications.[135]

Return data flows

The Unit has started to automate the process for the transmission of return data flows to reporting entities as well as data on the outcomes of the reports analysed, with the dual objective of increasing the efficiency of internal working processes and ensuring that confidential data are protected under the new legislative framework. This

[134] See Sections 8.1 and 9.1.
[135] See Section 1.3.1.

means no longer forwarding the reports on the outcomes of the analyses via certified mail alone but also using the special platform for transmitting STRs, in order to utilize existing IT channels and the related safeguards.

The first phase of the project, which was completed in 2017, regarded feedback on the STRs which, following analyses conducted by the UIF and the findings received by the investigative bodies, do not present sufficient elements to support suspicions of money laundering or the financing of terrorism. In subsequent phases this automatic forwarding function will be extended to other kinds of communications, in particular to those on the reports for which the analyses yielded positive results.

Exchange of confidential information

As part of the UIF's strategic plan, a project has been launched for the exchange of information with reporting entities aimed at raising security standards for information flows between the UIF and the obliged entities when analysing STRs (which often requires the procurement of additional documentation compared with that provided in the reports). Another objective is the standardization and restructuring of the format for exchanging information in order to facilitate and make more effective the incorporation of the data into the body of information available to the Unit.

Taking account of the complexity of this activity, the project was subdivided into two phases designed to achieve these two objectives. The first phase will enable the requests for information and related responses to be channelled in ways that raise security levels and protect the confidentiality of the information exchanged. The next phase will focus on creating a standard data format that will enable intermediaries and other reporting entities to reduce response times and the related costs and will allow the Unit to integrate the information received into its own IT systems more effectively.

Automatic classification of reports

In recent years the continuous and vigorous growth in the availability of unstructured data on the internet has spurred scientific research to study new mechanisms, automated to the greatest degree possible, for identifying, classifying and interpreting information. This is what the technology behind semantic engines aims to do: to extract knowledge from high volumes of unstructured data (such as documents, e-mails, social media and so on).

Among the most promising areas in this field are those of machine learning and deep learning, designed to construct forecasting models capable of making choices based on the data and not on static IT instructions.

The FIU, with the support of the Bank of Italy's IT function, has conducted a number of trials using open-source deep-learning engines to verify their applicability to STR classification.

The project seeks to develop an engine which, after an initial 'training' period in which STRs already examined by experts are analysed, is then able to independently classify them from a number of perspectives (i.e. rating or assignment to a category). This automatic classification should aid first-level analysis and speed up the preparatory work for processing the reports.

Management of the registry of reporting entities

Work is under way on a project to improve how the reporting entities' registry is managed (i.e. of the entities that supply the various data flows to the Unit) to make it easier to update AML Officer data and to capture the main events affecting these entities (i.e. mergers, incorporations and liquidations).

Measures are being put in place to improve the matching between the names recorded in the different databases used by the UIF in order to reduce the number of doubtful pairings (which must be dealt with manually) by assigning a unique ID to the various names corresponding to one person or entity, thereby making it easier to use the information. The new system should improve the processing of foreign names (e.g. names written in Arabic or Chinese characters) which require different matching criteria from those used for Western scripts.

Improvement of personal data matching

10.5. External communication

The UIF is increasingly engaged in dialogue with the public at large and all other entities and institutions involved in preventing and combating money laundering and the financing of terrorism.

Communication with the public and the system

The Annual Report, through which the UIF informs the Government and Parliament and, indirectly, the general public of its activities, is officially presented every year to representatives of the institutions, financial intermediaries and operators at a public meeting.

The full Annual Report and its official presentation are both translated into English. The original Italian version and the English translation are both available on the UIF's website.[136]

Website

Over the course of 2017, the UIF's website[137] was updated to reflect new developments. In addition to describing its work, it provides an overview of the entire Italian and international anti-money laundering and counter-terrorism system, offering complete and up-to-date information on regulatory and institutional matters, projects and research. In 2016 a new section entitled 'Terrorist financing information portal' was added.[138]

Dialogue with obliged entities

The Unit continues to encourage and foster dialogue and meetings with representatives and members of the main categories of reporting entities. The objective is to raise awareness of the purposes and uses of the various types of reports received. This is done by providing feedback[139] that is also useful for making system-level comparisons, thereby facilitating more intensive dialogue with a view to ensuring more active cooperation.

Publications, presentations and seminars

To this end the UIF issues publications and its members participate in studies and research on regulations and scenarios for combating all types of financial crime.

The UIF continues to publish its Quaderni dell'antiriciclaggio, a series of notebooks on AML topics divided into two series: Dati statistici and Analisi e studi, which are prepared in both printed and electronic form. The first, published every six months, contains statistical data on the reports received and concise accounts of the Unit's activities. The second, inaugurated in March 2014, contains contributions in the

[136] https://uif.bancaditalia.it/pubblicazioni/rapporto-annuale/index.html.
[137] https://uif.bancaditalia.it/.
[138] https://uif.bancaditalia.it/adempimenti-operatori/portale-contrasto/index.html.
[139] See Section 2.3.

fields of anti-money laundering and the fight against terrorist financing. This last series, published in July 2017, included issue No. 8 of the Quaderni on money laundering from a penal and administrative perspective,[140] while in January 2018, issue No. 9 was published containing guidelines on the new AML regulation in the gaming sector.[141]

In 2017, the FIU took part in conferences, seminars and meetings to enhance awareness and understanding among the public, market operators and other authorities involved in the fight against money laundering and the financing of terrorism.

The Unit provided speakers at more than 40 training programmes for other authorities and trade associations, at both national and international level; among these events, of particular importance were the lessons given by the UIF at courses organized by the school for training officials at the Presidency of the Council of Ministers and the Finance Police and Carabinieri Academies (Scuola di polizia tributaria della Guardia di Finanza and Istituto Superiore dei Carabinieri). Again in 2017, the Unit took part in a series of training courses at the Scuola di Polizia Tributaria for officials from foreign countries. The UIF continued to work in tandem with Italy's universities, in particular the Bocconi University of Milan. Last year also saw continued and intensive participation by UIF staff members at some of the highest profile events in Italy and abroad held on issues of institutional relevance at which the Unit's studies were presented and its main modus operandi illustrated.[142]

[140] http://uif.bancaditalia.it/pubblicazioni/quaderni/2017/quaderni-8-2017/index.html
[141] http://uif.bancaditalia.it/pubblicazioni/quaderni/2018/index.html
[142] See Section 6.2.

ACTIVITIES

Information gathering

- 93,820 suspicious transaction reports received
- 102,060,572 aggregate data received
- 39,677 monthly 'ex post' declarations on gold transactions
- 962 'ex ante' declarations on gold transactions

Analysis and dissemination

- 94,018 suspicious transaction reports examined
- 77,976 reports sent to investigative bodies for further inquiry, of which 41,071 assessed as 'high' or 'medium-high' risk

Cooperation with investigative bodies and national authorities

- 429 responses to requests from judicial author
- 115 crime reports
- 38 suspensions of suspicious transactions
- 85 'freezing of assets' orders in relation to financing of terrorism or threats to peace and international security

Other cooperation initiatives

- Cooperation with the Ministry of Economic Development in relation to the Investor Visa Committee for Italy
- Opinion provided to the Ministry of Justice concerning the codes of conduct drawn up by representatives of the entities in charge of combating crime
- Signing a memorandum of understanding between the UIF and the Public Prosecutor's Office of Milan (27 January 2017), of Rome (9 May 2017) and of Naples (5 April 2018)
- Signing a memorandum of understanding with China's Anti-Money Laundering Monitoring and Analysis Center (20 June 2017)
- Signing a memorandum of understanding with the Anti-Mafia Investigation Department, the Finance Police and the State Police (5 October 2017)
- Signing a memorandum of understanding with the National Anti-Mafia Directorate (8 May 2018)

Cooperation with other FIUs

- 2,246 requests and spontaneous communications from FIUs in other countries
- 1,232 responses sent to FIUs in other countries
- 763 requests sent to FIUs in other countries

Raising awareness about money laundering and financing of terrorism

- Speakers at more than 40 conferences and workshops on money laundering at universities and other institutions
- Speakers at workshops for trainee magistrates, organized by the Scuola Superiore della Magistratura
- 3 contributions to the *Analisi e studi* series of the publication *Quaderni dell'antiriciclaggio*

Regulatory activity

- Communication on countering international financing of terrorism (13 October 2017)
- Communication regarding the implementation of Legislative Decree 90/2017 transposing the Fourth AML Directive (4 July 2017)

Upgrading the IT infrastructure

- Introduction of the system for managing data exchanges with judicial authorities and foreign FIUs with greater automation in the management of external requests
- Launch of activities to complete the IT system for collecting and using threshold-based communications
- Development of the project to automate the transmission of return information flows to reporting entities
- Fine tuning to strengthen internal security and the mechanisms for the traceability of access as part of the protection of sensitive data used to achieve institutional objectives

GLOSSARY

Accredited entities and agents

Pursuant to Article 1(2)(nn) of Legislative Decree 231/2007, they are accredited operators or agents, of any kind, other than the financial agents listed on the register under Article 128-quater, paragraphs 2 and 6 of the TUB, used by payment service providers and electronic money institutions, including those with their registered office and head office in another Member State, to carry out their activities on Italian national territory.

Administrations and bodies concerned

Pursuant to Article 1(2)(a) of Legislative Decree 231/2007, they are the bodies responsible for supervising obliged entities not supervised by the relevant authorities, namely government departments, including tax offices, those with powers of inspection or authorized to grant concessions, authorizations, licences or other permits, of any kind, and the bodies responsible for verifying the possession of the requisites of professionalism and integrity, under the relevant sectoral rules. For the exclusive purposes of the abovementioned decree, the definition of administrations concerned includes the Ministry of Economy and Finance as the authority responsible for supervising auditors and auditing firms with no mandate to audit public-interest entities or bodies under an intermediate regime, and the Ministry of Economic Development as the authority responsible for supervising trust companies not listed on the register under Article 106 of the TUB.

Anti-Mafia Investigation Department (Direzione Investigativa Antimafia - DIA)

A specialized interforce investigation bureau drawn from various police forces and having jurisdiction over the entire national territory. Created under the Interior Ministry's Public Security Department by Law 410/1991, the Department has the exclusive task of coordinating investigations into organized crime, in all of its forms and connections, and also carrying out police enquiries into crimes of mafia-style criminal association or crimes related thereto.

Beneficial owner

Pursuant to Article 1(2)(pp) of Legislative Decree 231/2007, the beneficial owner (or owners) is the natural person, other than the customer, who is the ultimate beneficiary on whose behalf the ongoing relationship is established, the professional service is provided or the transaction is carried out.

Central contact point

Pursuant to Article 1(2)(ii) of Legislative Decree 231/2007, this is a person or department, established in Italy, designated by the electronic money institutions, as defined in Article 2(1)(3) of Directive 2009/110/EC, and by payment service providers, as defined by Article 4(11), of Directive 2015/2366/EC, with their registered office and head office in another Member State, and that operates, without a branch office, on national territory via accredited entities and agents.

Economic and Financial Affairs Council (ECOFIN)

The Economic and Financial Affairs Council is a configuration of the Council of the European Union (the Council of the European Union is a single legal entity but it meets in ten different 'configurations' depending on the subject matter discussed). ECOFIN is made up of the economics and finance ministers of all member states and, on occasion, national budget ministers. It meets once a month and is responsible for economic policy, taxation matters, financial markets and capital movements, and economic relations with countries outside the EU. It prepares and, together with the European Parliament, adopts the EU's annual budget and coordinates EU positions for international meetings, such as the G20, the International Monetary Fund and the World Bank. It is also responsible for the financial aspects of international negotiations on measures to tackle climate change.

Egmont Group

An informal organization formed in 1995 by a group of FIUs to further international cooperation and enhance its benefits. The number of member FIUs has grown steadily. In 2010 the Group became a formal international organization; its secretariat is in Toronto.

European FIU Platform

An EU body chaired by the European Commission and composed of the EU FIUs. Article 51 of the Fourth AML Directive formally recognized the role of the platform, in operation since 2006, and described its mandate in terms of developing stronger cooperation, exchanging opinions, and providing assistance in matters relating to the implementation of EU rules that apply to FIUs and reporting entities.

European Union countries

These comprise the 15 countries that were member states of the European Union prior to May 2004 (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom) and the 13 new member states admitted since then (Bulgaria, Cyprus, Croatia, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia and Slovenia).

Financial Action Task Force (FATF)

An intergovernmental organization within the OECD whose purpose is to develop and promote strategies for countering money laundering and terrorist financing at national and international level. Its decisions are approved by the OECD. During its initial mandate, beginning in 1989, the Task Force issued the Forty Recommendations on monitoring money laundering; during subsequent mandates, 9 Special Recommendations on international terrorist financing were added. The matter was thoroughly reviewed in 2012 with the issue of the revised Forty Recommendations. The FATF also promotes the extension of anti-money laundering and counter-terrorism measures beyond the OECD's membership, cooperating with other international organizations and conducting inquiries into emerging trends and money laundering typologies.

Financial Intelligence Unit (FIU)

A central, national unit assigned, for the purpose of combating money laundering and the financing of terrorism, to receive and analyse suspicious transaction reports and other information relevant to money laundering, terrorist financing and their predicate crimes and to disseminate the results of such analyses. Depending on the choices of national legislatures, the FIU may be an administrative authority, a specialized structure within a police force, or part of the judicial authority. In some countries a mix of these models has been adopted.

Financial Security Committee (FSC) Comitato di Sicurezza Finanziaria

Under Article 3 of Legislative Decree 109/2007, this is a committee formed at the Ministry of Economy and Finance (MEF), chaired by the Director General of the Treasury, composed of 15 members and their respective delegates, appointed by MEF decree, upon designation by the Minister of the Interior, the Minister of Justice, the Minister of Foreign Affairs and International Cooperation, the Minister of Economic Development, the Bank of Italy, CONSOB, ISVAP (now IVASS) and the Financial Intelligence Unit. The Committee also includes a manager from the MEF, a Finance Police Officer, a manager or police officer of an equivalent rank under Article 16 of Law 121/1981, in the service of the Anti-Mafia Investigation Department, an officer of the Carabinieri, a manager from the Customs and Monopolies Agency and a magistrate from the National Anti-Mafia Directorate. For asset freezes, the Committee is supplemented by a representative of the state property agency. The entities represented on the FSC shall communicate to the Committee, even derogating from official secrecy, the information in their possession relevant to matters within the Committee's remit. In addition, the judicial authorities shall transmit all information deemed useful for combating the financing of terrorism and the proliferation of weapons of mass destruction. The entry into force of Legislative Decree 231/2007 extended the Committee's remit, initially limited to the coordination of action against the financing of terrorism, to the fight against money laundering (See Article 5(3) of Legislative Decree 231/2007 previously in force, which now corresponds to Article 5 paragraphs 5, 6 and 7).

Financing of terrorism

Under Article 1(1)(d) of Legislative Decree 109/2007, the financing of terrorism is any activity directed, by whatever means, to the supply, intermediation, deposit, custody or disbursement of funds or economic resources, however effected, which are destined, in whole or in part, to be used for the commission of

one or more crimes for the purposes of terrorism as specified in the Penal Code, regardless of the actual utilization of the funds or economic resources for the commission of such crimes.

FIU.NET

A communications infrastructure among the Financial Intelligence Units of the European Union permitting a structured, multilateral interchange of data and information, with standardized applications and immediate and secure data exchange.

Freezing of Assets

Under Legislative Decree 109/2007, Article 1(1)(e), this is a prohibition on the movement, transfer, modification, utilization or management of funds or access to funds so as to modify their volume, amount, location, ownership, possession, nature or destination, or any other change that permits the use of the funds, including portfolio management.

General government entities

Pursuant to Article 1(2)(hh) of Legislative Decree 231/2007, these are general government entities under Article 1(2) of Legislative Decree 165/2001, and subsequent amendments, national public bodies, and companies owned and controlled by general government entities, pursuant to Article 2359 of the Italian Civil Code, limited to their activities of public interest, governed by national or EU law, as well as parties responsible for tax collection at national or local level, regardless of the legal form.

High-risk third countries

Pursuant to Article 1(2)(bb), Legislative Decree 231/2007, these are non-EU countries whose systems have strategic deficiencies in their national AML/CFT regimes, as identified by the European Commission, with its delegated Regulation (EU) 2016/1675 and subsequent amendments, in the exercise of its powers under Articles 9 and 64 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015.

Means of payment

Pursuant to Legislative Decree 231/2007, Article 1(2)(i), means of payment are cash, bank and postal cheques, banker's drafts and the like, postal money orders, credit transfers and payment orders, credit cards and other payment cards, transferable insurance policies, pawn tickets and every other instrument available making it possible to transfer, move or acquire, including by electronic means, funds, valuables or financial balances.

Money laundering

Article 648-bis of the Penal Code makes punishable for the crime of money laundering anyone who, aside from cases of complicity in the predicate crime, 'substitutes or transfers money, assets or other benefits deriving from a crime other than negligence, or who carries out in relation to them other transactions in such a way as to hamper the detection of their criminal provenance.' Article 648-ter makes punishable for illegal investment anyone who, aside from the cases of complicity in the predicate crime and the cases specified in Article 648 and 648-bis, 'invests in economic or financial assets moneys, goods or other assets deriving from crime.'

Pursuant to Legislative Decree 231/2007, Article 2(1), the following actions, if performed intentionally, constitute money laundering: '(a) the conversion or transfer of property, carried out knowing that it constitutes the proceeds of criminal activity or of participation therein with the aim of hiding or dissimulating the illicit origin of the property or of helping any individual involved in such activity to avoid the legal consequences of his or her actions; (b) hiding or dissimulating the real nature, origin, location, arrangement, transfer or ownership of property or rights thereto, carried out in the knowledge that they constitute the proceeds of criminal activity or of participation therein; (c) the acquisition, detention or use of property, knowing at the time of receiving it that it constitutes the proceeds of criminal activity or of participation therein; and (d) participation in one of the actions referred to in the preceding subparagraphs, association with others to perform such actions, attempts to perform them, the act of helping, instigating or advising someone to perform them or the fact of facilitating their performance.'

Moneyval (Select Committee of experts on the evaluation of anti-money laundering measures)

Moneyval is a sub-committee of the European Committee on Crime Problems (CDPC) formed by the Council of Europe in September 1997. It serves as the Council's unit on money laundering, also taking account of FATF measures, making specific recommendations to the member states. It evaluates the measures on money laundering taken by the Council members that are not FATF members. As a regional grouping, it has the status of an Associate Member of FATF.

Under a thoroughly revised statute, since January 2011 Moneyval has served as an independent monitoring body of the Council of Europe in the fight against money laundering and terrorist financing; it reports directly to the Committee of Ministers, to which it submits an annual report.

Office of Foreign Assets Control (OFAC)

Under the US Treasury Department, the Office was established under the auspices of the Undersecretary of the Treasury for terrorism and financial intelligence. OFAC governs and applies economic and trade sanctions ordered against foreign nations, organizations and individuals as part of US foreign and security policy.

Organization of Agents and Mediators (Organismo degli Agenti e dei Mediatori - OAM)

Pursuant to Article 1(1)(q) of Legislative Decree 231/2007, this Organization is responsible for managing the lists of financial agents and brokers, pursuant to Article 128-undecies of the TUB (Consolidated Law on Banking). The OAM also holds: i) the currency exchange register which has a special section for providers of virtual currency services (Article 17-bis, paragraph 8-bis, Legislative Decree 141/2010, added by Legislative Decree 90/2017); ii) the register of entities and agents under Article 45 of Legislative Decree 231/2007; and iii) the register of cash-for-gold traders under Article 1(1)(q) of Legislative Decree 92/2017.

Politically exposed persons (PEPs)

Pursuant to Article 1(2)(dd) of Legislative Decree 231/2007, these are natural persons that currently hold, or held important public offices up until less than one year ago, together with their immediate family members or persons known to be their close associates, and are listed as follows: 1) natural persons that hold or have held important public offices and are or have been: President of the Italian Republic, Prime Minister, Minister, Deputy Minister and Undersecretary, Regional President, Regional minister, Mayor of a provincial capital or metropolitan city, Mayor of a town with not less than 15,000 inhabitants, and similar positions in foreign countries; 1.2 member of parliament, senator, European M.P., regional councillor, and similar positions in foreign countries; 1.3 a member of a central management bodies of political parties; 1.4 a Constitutional Court judge, a magistrate of the Court of Cassation or the Court of Auditors, a State Councillor or other component of the Administrative Justice Council for the region of Sicily, and similar positions in foreign countries; 1.5 a member of the decision-making bodies of central banks and independent authorities; 1.6 an ambassador, a chargé d'affaires or equivalent positions in foreign states, high-ranking officers in the armed forces or similar ranks in foreign countries; 1.7 a member of the administrative, management or supervisory bodies of enterprises owned, also indirectly, by the Italian State or by a foreign State or owned, mainly or totally, by the regions, provincial capitals and metropolitan cities and by towns with a total population of not less than 15,000 inhabitants; 1.8 a general manager of an ASL (Local Health Authority) or a hospital or university hospital or other national health service entities; and 1.9 a director, deputy director, member of a management board or a person with an equivalent role in international organizations; 2) family members of PEPs include: the parents, the spouse or any person considered by national law as equivalent to the spouse, the children and their spouses or partners considered by national law as equivalent to the spouse; 3) persons who are known to be close associates of politically exposed persons include: 3.1 natural persons linked to PEPs because they have joint beneficial ownership of legal entities or other close business relations; and 3.2 natural persons that only formally hold total control of an entity known to have been set up for the de facto benefit of a PEP.

Sectoral supervisory authorities

Pursuant to Article 1(2)(c) of Legislative Decree. 231/2007, the Bank of Italy, CONSOB and IVASS are the authorities designated for supervising and checking banking and financial intermediaries, auditors and auditing firms with mandates to audit public-interest entities and entities under an intermediate regime;

the Bank of Italy supervises and checks non-financial operators with cash-in-transit and valuable items transport companies that employ qualified private security guards, and that have a licence under Article 134 of the TULPS (Consolidated Law on Public Security), limited to the handling of euro banknotes under Article 8 of Decree Law 25 September 350/ 2001, converted with amendments into Law 409/2001.

Self-laundering

Pursuant to Article 648-ter.1 of the Penal Code, 'whoever, having committed or attempted to commit a crime with criminal intent, uses, replaces or transfers money, assets or other utilities deriving from the commission of such a crime to economic, financial, entrepreneurial or speculative activities, in such a way as to actively hinder detection of their criminal origin' can be punished for the crime of self-laundering. The rule was introduced by Article 3(3) of Law 186/2014.

Self-regulatory body (SRB)

Pursuant to Article 1(2)(aa) of Legislative Decree 231/2007, this is a body that represents a professional category, including its various branches and the disciplinary boards on which the current legislation confers regulatory powers, supervisory powers, including checking compliance with the rules governing the exercise of the profession and the imposition, via the mechanisms in place for this purpose, of the sanctions applicable for the violation of such rules.

Single Electronic Archive (Archivio unico informatico - AUI)

Pursuant to Article 1(2)(b) of Legislative Decree 231/2007, which was in force before Legislative Decree 90/2017 was issued, the Single Electronic Archive is a database created and run using IT systems that provide for the centralized storage of all the information acquired in fulfilling the identification and regulation obligations in accordance with the principles laid down in the decree and the measures issued by the Bank of Italy.

Special Foreign Exchange Unit (Nucleo Speciale di Polizia Valutaria - NSPV)

Formed within the Finance Police, the unit combats money laundering, both as an investigative police body and as the administrative body responsible, together with the Bank of Italy and the Anti-Mafia Investigation Department, for controls on the financial intermediation sector. The law confers special powers relating to foreign exchange regulations on the Unit's members, as well as those concerning fiscal powers.

Tax havens and/or non-cooperative countries and territories

The blacklist of jurisdictions named in the decree of the Minister of Finance of 4 May 1999 (most recently amended by the ministerial decree of 12 February 2014). The decrees of the Minister of Economy and Finance of 23 January 2002 and of 21 November 2001 no longer apply because the relevant articles of the Consolidated Income Tax Law (TUIR) providing for it were repealed or amended. The blacklist comprises the following jurisdictions: Abu Dhabi, Ajman, Andorra, Anguilla, Antigua and Barbuda, Aruba, the Bahamas, Bahrein, Barbados, Belize, Bermuda, Bonaire, the British Virgin Islands, Brunei, the Cayman Islands, the Cook Islands, Costa Rica, Curaçao, Djibouti (formerly the Afars and Issas), Dominica, Dubai, Ecuador, French Polynesia, Fuijairah, Gibraltar, Grenada, Guatemala Guernsey, Hong Kong, Isle of Man, Jersey, Kiribati, Lebanon, Liberia, Liechtenstein, Macao, the Maldives, Malaysia, the Marshall Islands, Mauritius, Monaco, Monserrat, Nauru, Niue, New Caledonia, Oman, Panama, the Philippines, Ras El Khaimah, Saint Helena, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, the Seychelles, Sharjah, Singapore, Sint Eustatius and Saba, Sint Maarten (the Dutch part only), the Solomon Islands, Switzerland, Taiwan, Tonga, the Turks and Caicos Islands, Tuvalu, Umm Al Qaiwain, Uruguay and Vanuatu. In addition, the blacklist includes the countries that are not compliant with the rules against money laundering and terrorist financing, according to the FATF's 'Public Statement February 2017' and 'Improving Global AML/CFT compliance: On-going process February 2017': Afghanistan, Bosnia and Herzegovina, North Korea, Ethiopia, Guyana Iran, Iraq, Laos, Myanmar, Papua New Guinea Syria, Uganda, Vanuatu and, Yemen. The list also includes high-risk third countries, identified in compliance with the Fourth AML Directive.

Virtual currency

Pursuant to Article 1(2)(qq) of Legislative Decree 231/2007, 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, used as a medium of exchange for purchasing goods and services, and transferred, stored and traded electronically.

ACRONYMS AND ABBREVIATIONS

ANAC	National Anti-Corruption Authority (Autorità Nazionale Anticorruzione)
ATM	Automated Teller Machine
AUI	Single Electronic Database (Archivio Unico Informatico)
CASA	Anti-Terrorism Strategic Analysis Committee (Comitato di Analisi Strategica Antiterrorismo)
CDP	Cassa Depositi e Prestiti SpA
CIFG	Counter-ISIL Finance Group
CNDCEC	National Council of the Order of Accountants and Bookkeepers (Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili)
CNF	(National Lawyers' Council) Consiglio Nazionale Forense
CNN	National Council of Notaries (Consiglio Nazionale del Notariato)
CONSOB	Companies and Stock Exchange Commission (Commissione Nazionale per le Società e la Borsa)
DDA	Anti-Mafia District Directorate (Direzione Distrettuale Antimafia)
DIA	Anti-Mafia Investigation Department (Direzione Investigativa Antimafia)
DNA	National Anti-Mafia Directorate (Direzione Nazionale Antimafia e Antiterrorismo)
ECB	European Central Bank
ECOFIN	Economic and Financial Affairs Council
ELMI	Electronic Money Institutions
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSC	Financial Security Committee
ISIL	Islamic State of Iraq and the Levant
IVASS	Insurance Supervisory Authority (Istituto per la Vigilanza sulle Assicurazioni)
MEF	Ministry of Economy and Finance

NRA	National Risk Assessment
NSPV	Special Foreign Exchange Unit of the Finance Police (Nucleo Speciale di Polizia Valutaria della Guardia di Finanza)
OAM	Organization of Agents and Mediators (Organismo degli Agenti e dei Mediatori)
OECD	Organization for Economic Cooperation and Development
PEP	Politically Exposed Person
PI	Payment Institution
RADAR	Collection and Analysis of AML Data (Raccolta e Analisi Dati AntiRiciclaggio)
SARA	Aggregate AML Reports (Segnalazioni AntiRiciclaggio Aggregate)
STR	Suspicious Transaction Report
TUB	Consolidated Law on Banking (Testo Unico Bancario – Legislative Decree 385/1993)
TUF	Consolidated Law on Finance (Testo Unico della Finanza – Legislative Decree 58/1998)
TUIR	Consolidated Law on Income Tax (Testo Unico delle Imposte sui Redditi – Decree of the Presidential Republic 917/1986)
UIF	Italy's Financial Intelligence Unit (Unità di Informazione Finanziaria)
UNCAC	United Nations Convention against Corruption
VAT	Value-Added Tax