POLITECNICO DI TORINO

Corso di Laurea Magistrale
in Ingegneria Gestionale

Tesi di Laurea Magistrale

Anti Financial Crime transaction monitoring in correspondent banking: new regulatory expectations and technical challenges

Relatore
Prof. Carlo Cambini

Candidata
Emma Lombardi
s302491

Tutor aziendale
Dario Moncalvo, PhD

Anno Accademico 2022-2023

Summary

Money laundering is the process through which criminals introduce illicit funds into the legal economy. Anti-Money Laundering (AML), along with Combating the Financing of Terrorism (CFT), is an ongoing activity to which all financial intermediaries are subjected due to national law and international guidelines.
One specific aspect of this broader activity is Transaction Monitoring. This thesis, developed in collaboration with the Models, Analytics and Special Investigation office of Intesa Sanpaolo Group, proposes the development of a proprietary algorithm to monitor the wire transfers activity of its customers. The aim is to address the challenges affecting the entire chain of this operational activity and, as a final step, enhance the productivity of the output sent to the Italian Financial Intelligence Unit (UIF).
Starting with a description of the national and international anti-money laundering legislative landscape, moving on to the technical explanation of what a wire transfer is and the tools for moving funds internationally (Correspondent Banking), the thesis then highlights various issues within the current system to propose a solution. The work concludes with potential and future project implementations.

Table of Contents

List of Tables

List of Figures

Preface and Information security disclaimer

The current dissertation steams from the intra-curricular internship that I had the opportunity to undertake from 31/07/2023 to 14/11/2023 in Intesa Sanpaolo. During this period, I fully joined the Models, Analytics and Special Investigations team, namely MAS, of the Anti Financial Crime Central Directorate of the Intesa Sanpaolo Group.
This experience allow me to be exposed to a variety of privileged information and know-how that are not publicly disclosed.
While this situation was an unparallel forging experience to approach both the financial sector as well as the anti financial crime professional niche, it has very severe limitations in terms of data and information contents that may be reported outside its boundaries.
The current dissertation reflects those limitations, even if its subject is approached, at least in the initial part, in terms that are not referred to the internship experience but are pertinent to the entire financial industry setting. In the last part, some more direct linkage to the internship tasks is apparent while protected by a careful selection of reported information that prevent to disclose any sensitive detail.

Chapter 1

Introduction to Anti Financial Crime transaction monitoring

1.1 What is Money Laundering

Money laundering is the process of "cleaning" illicitly obtained funds, typically stemming from illegal activities, in order to use them within the legitimate economy. Examples of unlawful activities that necessitate money laundering include drug trafficking, arms sales, fraud, prostitution, or embezzlement. Money laundering is, in all respects, a criminal act and should be analyzed as an activity pursued to accumulate wealth rapidly and abundantly, often disregarding social consequences. Quantifying the economic damage resulting from money laundering is challenging due to the clandestine nature of the activity. According to Europol [1], estimates suggest that the economic loss amounts to between 2% and 5% per year of the GDP.
Traditionally, money laundering could be broken down into three processes that recur in every money laundering scheme: placement, layering, and integration.

Placement is the stage where illicit funds are introduced into the economic system in various forms with the purpose of making them usable. Some of the methods used in this stage include the use of fake documents, money transportation, currency exchange or even converting the money into gold, which can be sold for cash in many countries. The common denominator underlying these processes is deception. [2]

In the *layering* phase, the money is moved to obscure its origins. For instance, if real estate was acquired during the placement phase, it is sold through legal means in the layering phase. Dealing with different jurisdictions eases this process, as the incongruity of laws and structures increases the complexity of tracing a linear path for the funds. The layering phase often involves financial systems with fewer Anti Money Laundering (AML) controls and less collaboration with international authorities. [3, 4]
The layering process involves activities such as investments in highly liquid financial products, donations, or money transfers to so-called shell companies. [3] A shell company is a virtual organization with minimal physical presence and lacks substance or a genuine commercial purpose. These entities are often located in countries with preferential tax systems, often referred to as tax havens.

Finally, the *integration* phase involves reintroducing the illicit funds into the economy by using them for legal activities such as investments. The goal is to merge the funds in a manner that avoids suspicion and gives the appearance of legitimacy. To achieve this, criminals often engage in cash-intensive businesses like bars, restaurants, and nightclubs.[2, 5]

1.2 How the world fights Money Laudering

As Money Laundering is a pervasive process embedded in any crime with an economic purpose, it is a global threat for human societies not limited by any border. On the contrary, there are significant differences in the Anti Money Laundering regulatory frameworks across different jurisdictions and chiefly from their continental clustering (US, EU, APAC, etc.). Such disomogeneus mosaic is apparent observing that those involved in anti-money laundering offenses are well acquainted with the strengths and weaknesses of the system within which they operate, defined as the legislative framework of each country and, more broadly, of any jurisdiction. A detailed understanding of how these systems operate allows them to select the most accommodating context for their purposes each time.
The absence of a single authority at the supra-national level makes it challenging to correct the mechanisms that incentivize downward behavior.
In order to address this asymmetry that favors those seeking to engage in money laundering-related activities, efforts have increasingly been made over time to bluid up a global network aimed at coordinating, facilitating, and enhancing the fight against this phenomenon.[6]

Money laundering thus begins to gain recognition in international sources, which, since the late '80s, have extended the fight against serious crimes to the downstream

phase of the production and use of illicit proceeds.
Starting from a focused approach on the cash money steaming from drug trafficking on international scale ("follow the money") in order to detect and dismantle criminal relationships and networks, the Anti Money Laundering (AML) system has grown to the extent of including many other traditional criminal offences. More recently, from general AML provisions have been distinguished specific actions against the financial feeding of terrorist groups that, generally, are clustered in the Counter Terrorism Financing (CFT) term.
The field of prevention and combating money laundering becomes specialized and acquires its own identity; a multidisciplinary and complex sector emerges, rich in connections with various others, ranging from criminal to banking, financial and tax-related areas.
The upcoming chapters will delve into how various jurisdictions and, more broadly, the entire global community have organized themselves to coordinate efforts in addressing Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT).

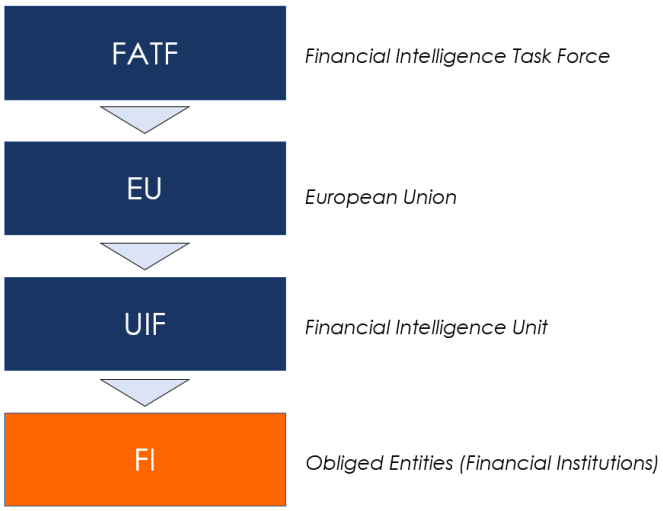

Figure 1.1: Anti Financial Crime macro organization

1.3 International standards on AML/CFT: the role of the FATF

The Financial Action Task Force, known worldwide as FATF, plays a pivotal role in the global landscape of anti-money laundering efforts. GAFI, in its original French

name, was founded on 1989 on the initiative of G7 with the idea of developing policies to combat money laundering (Anti Money Laundering). In 2001 his mandate was expanded with the activity of countering the financing of terrorism. [7, 8]
The FATF is a globally recognized supranational organization primarily responsible for the development and dissemination of standards for the prevention and combat of money laundering, terrorist financing, and proliferation. It enjoys alignment from both other international bodies and individual nation-states, subjecting the latter to scrutiny to ensure the correct and effective implementation of these standards in these entities.

The main activities of the FATF revolve around updating the "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation", encompassing the 40 recommendations. These activities also include the "Mutual Evaluation" process and the publication of "Methods and Trends."

Recommendations

First published in 2012 and subject to annual review and supplementation, the 40 Recommendations represent the most comprehensive instrument of soft law to which every legal system adheres in the development of Anti Money Laundering and Counter the Financing of Terrorism legislation[9].

The 40 Recommendations are divided into seven distinct areas:

- A - AML/CFT Policies and coordination (1-2)
- B - Money laundering and confiscation (3-4)
- C - Terrorist financing and financing of proliferation (5-8)
- D - Preventive measures (9-23)
- E - Transparency and beneficial ownership of legal persons and arrangements (24-25)
- F - Powers and responsibilities of competent authorities and other institutional measures (26-35)
- G - International cooperation (36-40)

Group A, focused on policy and coordination, suggests that countries should conduct an assessment of their domestic money laundering and terrorism financing threats. They should then employ a risk-based approach (RBA) to mitigate these

risks effectively, ensuring that the measures taken align with the identified threats.

Group B, extends the application of money laundering laws to cover the proceeds of any criminal activity. They should also empower competent authorities to freeze or seize assets that are subject to charges related to money laundering.

Group C focuses on Countering the Financing of Terrorism (CFT) and the proliferation of weapons. It recommends that countries should categorize activities associated with terrorism as financial crimes, even if they are not directly linked to a specific terrorist act.

Group D deals with preventive measures and contains multiple recommendations. Among them, it is worth highlighting that Recommendation 10 is the one concerning the Customer Due Diligence (CDD), a series of precautionary measures that financial institutions should take to ensure the identity of their customers. In particular, a financial institution should identify the customers - either if it is a natural or legal person - and take reasonable steps to confirm their identity, be aware of their businesses and risk profiles, and conduct ongoing procedures during the relationship to ensure they are in line with the institution's ethics.
Also significant are Recommendations 12 to 16, about additional measures for specific customers and activities. Recommendation 13, in particular, lists additional due diligence when being involved in correspondent banking businesses (chapter 3 will go deeper into this) and Recommendation 16 requires complete information when using wire transfers to move funds.
From 17 to 19, instead, are Recommendations on reliance, controls and financial group concerning schema in which third parties or High Risk Geographies are involved.

Group E encompasses two Recommendations (24-25) related to the transparency and beneficial ownership of legal entities and arrangements. These Recommendations advise countries to assess the potential misuse of these entities for financing terrorism or money laundering and to implement suitable measures to prevent such misuse.

Group F's Recommendations (26-35) outline the roles and responsibilities of competent authorities. Governments should employ supervisory bodies to oversee the compliance of obliged entities with FATF's Recommendations. These supervisory bodies should possess adequate independence, allowing them to conduct inspections, access all relevant records, compel data production, and enforce appropriate and dissuasive sanctions in cases of non-compliance. Among this group of Recommendation, the 29 is relevant for what this work concerns since it introduces

the role of the Financial intelligence units, which "serve as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering".

Group G addresses the aspect of international cooperation with Recommendations 36-40. With them, FATF emphasizes the importance of countries working together and offering mutual legal assistance.

The FATF Recommendations are commonly known as the FATF Standards. The document in which they are listed comprises the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary. For its part, the FATF continuously monitors new and evolving threats to the financial system and regularly updates and refines its Recommendations so that countries have up-to-date tools to go after criminals.
As countries have diverse legal, administrative and operational frameworks and different financial systems, they should adapt the Recommendations to their particular circumstances but the guiding principle that every country must follow is that of the risk-based approach which emphasizes the need for countries to identify and understand the money laundering and terrorist financing risks they are exposed to. To assist nations in applying its Standards, the FATF develops guidance documents and best practice papers on various topics. These resources are periodically updated to incorporate insights gained from both public authorities and the private sector, ensuring that countries can draw upon this collective experience to efficiently implement the FATF Recommendations within their unique national settings.
Despite the absence of "sanctions" in the strict sense, violations and deviations entail economic, reputational, and political risks and costs. Therefore, the incentive for the correct application of the standards stems from an assessment of "convenience" in which the advantages achievable through misalignment and the consequences of inspections are weighed.

Mutual evaluation

The implementation of the standards is subjected to comprehensive verification and evaluation programs. The FATF conducts Mutual Evaluations of its member countries, aptly named for their peer-review nature, carried out reciprocally by experts from other countries for each member state. These evaluations occur in successive cycles, with the aim of ensuring that interventions for each country are subsequent not too far apart in time.
During a mutual evaluation, the assessed country must demonstrate that it has an effective framework to protect the financial system from abuse.

Mutual Evaluations have two main components, effectiveness and technical compliance. The first consists in an on-site visit by a team of experts to the assessed country in which the country has to demonstrate its measures are working and delivering the right results.
The second one instead assessed the regulation framework of the country taken into account. In practice, the assessed country must provide information on the laws, regulations and any other legal instruments it has in place to combat money laundering and the financing of terrorism and proliferation. [7]

Methods and Trends

The FATF conducts research activities aimed at keeping its Standards up to date and, more broadly, to support its efforts in disseminating knowledge. This includes research on emerging methods and trends to help countries recognize, evaluate, and comprehend the risks associated with money laundering and terrorist financing. The analysis of continuously evolving criminal trends and methods, along with the assessment of strengths and weaknesses, serves as the foundation for updating standards. It guides the development of policies through guidelines, and provides insights to national authorities on risks and priorities.[7]

1.4 European regulatory framework

Acknowledging that Money Laundering and Terrorism Financing are supranational threats, the European Union has progressively established an articulated regulatory framework leveraging both Directives (to be adopted, translated and enforced by national law provisions) and Regulations (subject to direct application in Member states). This entanglement is supposed to balance the need for a coordinated and homogeneous approach to the matter with prerogatives and regulation peculiarities grounded in each country of the European Union.

Over the years, a full-fledged European anti-money laundering framework has taken shape, evolving in multiple directions. On the regulatory front, the structure is primarily defined through directives, from the first in 1991 to the fifth in 2018. Regulations and directives on specific matters are then grafted onto this primary framework.
Through these directives, European regulation has formulated a money laundering concept that, although lacking direct criminal relevance and developed as a prerequisite for the application of preventive measures, has promoted the alignment of incriminating definitions in EU to the international model outlined by FATF.[6, 10]

Now, delving into the specifics of the Directives:

First Directive (91/308/EEC of June 10, 1991): Published shortly after the Strasbourg Convention of the Council of Europe, it introduces the concept of money laundering, incorporating the definition of money laundering from the United Nations Vienna Convention of 1988.

Second Directive (2001/97/EC of December 4, 2001) effectively replaces its predecessor and substantially broadens the scope of criminal offenses by redefining "criminal activity." Furthermore, it expands the requirement to report suspicious transactions to encompass additional professionals, including auditors, external accountants, tax advisors, estate agents, notaries, and various independent legal experts. Additionally, this updated directive now encompasses a wider range of business sectors, including real estate firms, art dealers, retailers dealing in valuable items, and casinos, which could potentially be used for money laundering purposes.

Third Directive (EC 2005/60 of October 26, 2005) supersedes the two previous directives and aligns the scope of predicate offenses with "serious offenses." This directive offers more comprehensive guidelines and rules for the functioning of Financial Intelligence Units (FIUs) within EU member states, which enhances international cooperation and bolsters the efficacy of anti-money laundering efforts across Europe. Notably, it introduces the concept of a "risk-based approach", where the stringency of countermeasures is contingent upon the assessed risk of money laundering.

The Fourth Directive (EU 2015/849 of May 20, 2015) does not introduce significant changes in the definition and psychological elements of money laundering offenses. However, it expands the scope of "criminal activity" to include "tax crimes." Instead of completely replacing the previous directive, it amends and incorporates the third AML directive, enhancing existing measures and introducing new provisions. Notable changes include stricter requirements for revealing the beneficial owners of companies and fiduciary organizations, strengthened Customer Due Diligence (CDD) rules, and specific measures for politically exposed individuals (PEP). Reporting requirements for suspicious transactions become more rigorous, emphasizing greater cooperation between Financial Intelligence Units (FIU) of member states and the imposition of more severe sanctions for violations of AML regulations.

The Fifth Directive (EU 2018/843, dated May 30, 2018) builds upon the existing regulatory framework for anti-money laundering (AML) without substantially changing the definition of money laundering itself. This means that the Fourth AML Directive remains in effect, as some of its provisions are still relevant and can

be integrated into the Fifth Directive. The Fifth Directive introduces several new elements, including strengthened oversight by Competent Authorities over payment services and virtual currency providers, enhanced measures to counter terrorism financing, and the establishment of regulations for virtual currencies. Notably, it mandates more thorough and improved identification of cryptocurrency wallet holders. Additionally, the directive incorporates measures for monitoring high-risk transactions and provides authorities and Financial Intelligence Units (FIUs) with easier access to beneficial ownership registries.

Figure 1.2: Timeline of European Directives

1.4.1 New regulatory expectation: the AML Package

With the aim of enhancing the harmonization of regulatory systems across European countries, a comprehensive reform of European anti-money laundering legislation was initiated with the publication of the "AML Package" on July 20, 2021. The legislative package comprises four proposals by the European Commission (3 Regulations and a sixth Anti Money Laundering Directive).
To mitigate arbitrage and national incentives towards lower standards, the Package promotes a more harmonized and integrated system, primarily founded on a uniform "Rulebook" for operators in all countries and a significant restructuring of the institutional framework. This restructuring includes the establishment of a European Anti Money Laundering Authority (AMLA). [6, 11]

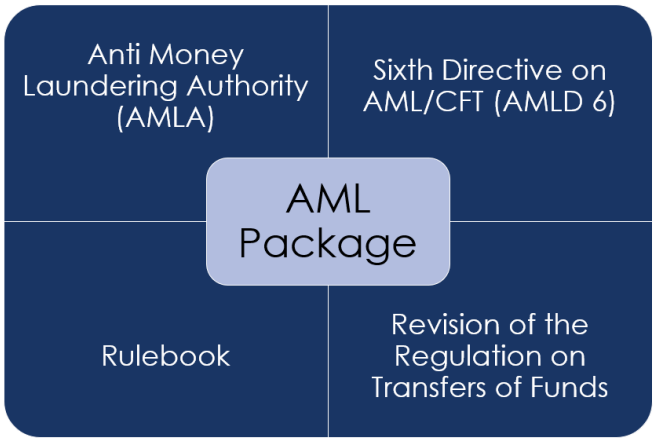

Figure 1.3: Contents of the AML Package

Of the four proposed documents, the only one already published and effective as of December 30, 2024, is the update on the fund transfer regulation.

New regulation on transfer of funds

This regulation amends Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or terrorist financing concerning data accompanying transfers of funds and certain crypto-assets. It introduces new provisions related to policies, procedures, and internal controls to ensure effective implementation if one of the providers of payment services or crypto-asset service providers has its registered office or is established within the European Union.
This regulation becomes effective as of December 30, 2024.
The three other innovations of the AML package have not been definitively published yet and are currently undergoing trilogue negotiations between the European Commission, the European Parliament, and the European Council.

Anti Money Laundering Authority (AMLA)

The new authority[12], known as the Anti Money Laundering Authority, replaces the AML/CFT oversight function that currently falls under the responsibilities of the European supervisory authorities (ESAs), which includes the European Bank Authority (EBA).
The insufficient control over the application of anti-money laundering rules by national entities, the inadequate detection of suspicious activities in cross-border contexts, and the inherent fragmentation within the organization of ESAs, which do not have AML/CFT as their sole focus, have led to scandals in recent years,

such as those involving Danske Bank and Wirecard.
For these reasons, there was a need for a single authority dedicated entirely to combating AML/CFT, equipped with the necessary tools to be more decisive and effective.

Regarding its functions, the Authority will be a legal entity in the form of a decentralized EU agency with responsibilities for rule and method convergence, coordination, and support for national authorities and direct supervision. In particular, AMLA will exercise two distinct roles.
Firstly, with the aim of centralizing supervision to provide a more uniform overview of dynamics involving multiple European states, by 2026, AMLA will directly supervise high-profile financial entities across the continent (previously the prerogative of national authorities and non-financial sector competences). To date, it is estimated that around 50 entities will fall under direct supervision. The guiding principle behind this framework is to have an authority whose scope and intervention mirror the operational perimeter of supervised financial entities.
In addition to direct supervision, AMLA will also conduct indirect supervision of other obliged entities in the financial sector through evaluations of the activities of different financial sector supervisors and non-financial sector surveillance through the verification of the activities of non-financial obliged entity supervisors.
As a second function, AMLA will coordinate the work of FIUs through the possibility for each national unit to delegate a member to the new authority. AMLA will be able to request "data and analysis" from FIUs for the purpose of assessing supranational risks, collect statistical data on the tasks and activities of FIUs, issue guidelines and recommendations, and promote joint analyses.
Furthermore, with the aim of improving communication and enhancing information exchange among various countries, the EuReCA database launched by EBA in 2022 will be transferred to the management of the AML Authority, thus centralizing knowledge and expediting interaction.[12]
Additionally, the new authority will conduct periodic reviews to ensure that countries have adequate resources to fulfill their obligations, may request direct inquiries from the underlying countries to carry out investigations using its own methods, or even serve as a channel of communication between intelligence units to conduct coordinated research.
To carry out all of these functions, AMLA will need to be financially self-sufficient and, for this purpose, will be funded by Europe for 25% and financial entities for 75%. AMLA's governance comprises two collective governing bodies (General Board and Executive Committee), along with the President and the Executive Director.
The General Board, composed of representatives from all member countries, will be responsible for deciding on guidelines and measures for obliged entities and FIUs. On the other hand, the Executive Committee will serve as the governing body

responsible for all decisions concerning obliged entities and competent authorities, including budget decisions and the day-to-day management of the authorities.

Anti Money Laundering Rulebook (AMLR)

The second document subjected to trilogues by the European Union aims to establish a set of rules designed to standardize the minimum standards within the EU for financial intermediaries to manage their AML/CFT compliance obligations. In detail, this document outlines a Rulebook, a unified regulatory framework that harmonizes the existing laws and ensures consistency and cohesion within the scope of application.
The most relevant provisions to be adopted under the AMLR pertain to control policies and procedures, group policies, branch offices in third countries, application and information for adequate verification, monitoring, and formats for Suspicious Activity Reports (SARs).

Anti Money Laundering Directive (AMLD 6)

The proposal for the Sixth Anti Money Laundering and Countering the Financing of Terrorism Directive (AMLD 6) replaces the current Directive (EU) 2015/849 (the Fourth AML/CFT Directive, which was amended by the Fifth Directive (EU) 2018/843).
Its purpose is to ensure greater convergence and consistency in the AML/CFT requirements applied by Member States and the activities carried out by supervisory authorities/FIUs. This takes into account the establishment of the AMLA while maintaining an adequate level of flexibility for individual Member States.
Provisions to be adopted under AMLD 6 cover topics such as the exchange of information by FIUs, the methodology for National Risk Assessment, joint supervision, the functioning of supervisory colleges, administrative sanctions, and the potential establishment of a central contact point.

1.5 Italian regulatory framework and Authorities

The Italian anti-money laundering framework has evolved in accordance with international standards and European directives. The legislative framework for anti-money laundering is represented by the Decree Law 21 November 2007 n. 231, which transposed European directives on this matter (2005/60/EC, (EU) 2015/849, (EU) 2018/843). Additionally, for aspects related to countering teh financing of terrorism and activities of countries threatening international peace and security, Decree Law 22 June 2007 n. 109, plays a significant role. These legislative texts

have been amended, most recently, by Decree Law 4 October 2019 n. 125, which included corrective measures and provisions for implementing the fifth anti-money laundering directive (2018/843). Further changes to the cash usage regime were introduced by Law 26 October 2019 n.124 , subsequently amended by the Law of 19 December 2019 n. 157.
The anti-money laundering prevention system relies on collaboration among operators, administrative authorities, investigative bodies, and judicial authorities. In the following paragraph the core institutional players acting in the Italian AML system are outlined.

Figure 1.4: Italian Anti Money Laundering framework

The *Minister of Economy and Finance*[1], as the technical expression of the legislative function, is responsible for the policies aimed at preventing the use of the financial and economic systems for money laundering from criminal activities

[1]https://www.mef.gov.it/index.html

or for financing terrorism. In order to implement these policies, the Ministry of Economy and Finance fosters collaboration among the Financial Intelligence Unit (FIU), sectoral supervisory authorities, professional associations, and law enforcement agencies, as well as between public entities and the private sector. The Ministry manages relations with European institutions and international bodies, monitors matters related to cash usage limitations, and exercises sanctioning powers, gathering relevant information from obligated entities, including through its own inspections.

The *Financial Security Committee (FSC)*[2],established by Legislative Decree 369/2001 (converted into Law 431/2001) within the Ministry of Economy and Finance, and regulated by Legislative Decree No. 109 of 2007, is responsible for developing the national analysis of money laundering and terrorist financing risks and strategies to counteract them. It exercises specific powers related to countering terrorist financing and activities of countries posing threats to international peace and security, as well as providing expert opinions.
The FSC is chaired by the Director General of the Treasury and has a comprehensive and diverse composition, including representatives from the Ministry of Economy and Finance, Ministry of the Interior, Ministry of Justice, Ministry of Foreign Affairs, Bank of Italy, National Commission for Companies and the Stock Exchange, Institute for the Supervision of Private Insurance and Pension Funds, Financial Intelligence Unit for Italy, Finance Guard, Anti-Mafia Investigative Directorate, Carabinieri Corps, and the National Anti-Mafia Directorate. Additionally, representatives designated by the Ministry of Economic Development and the Customs Agency are also part of it to address issues related to the proliferation of weapons of mass destruction.

Among the technical authorities, a central role is assigned to the *Financial Intelligence Unit for Italy (UIF)*[3], located within the Bank of Italy with autonomy and independence. The chosen approach aligns with international standards that allow countries to determine the set up of their intelligence unit within their own law enforcement structures or judicial bodies rather than within administrative authorities such as central banks or ministries.

Its primary functions are as follows[6]:

- Receiving and acquiring information regarding suspected money laundering and terrorist financing cases, primarily through reports of suspicious transactions submitted by intermediaries, professionals, and non-financial operators.

[2]https://www.dt.mef.gov.it/

[3]https://uif.bancaditalia.it/homepage/index.html

- Conducting financial analysis of this information, utilizing all available sources and powers, and assessing its relevance for transmission to the Special Currency Police Unit of the Finance Guard (NSPV) and the Anti-Mafia Investigative Directorate (DIA), the competent bodies for investigative inquiries. This analysis, favored by the legislator for this Authority over investigative activities, consists of a series of actions aimed at enriching the informational database of each report, identifying subjects and objective links, reconstructing financial flows, including transnational ones, and selecting cases characterized by higher risk.

- Performing strategic analysis, identifying trends, phenomena, as well as systemic vulnerabilities, and, for this purpose, utilizing information derived from the in-depth examination of reports of suspicious transactions, analysis of aggregated data, and any other relevant informational elements available to the Unit.

- Serving as the hub for international information exchange in the fight against money laundering and terrorist financing by activating the network of corresponding foreign authorities, the Financial Intelligence Units (FIUs), using dedicated channels and, when necessary, entering into specific protocols.

- Conducting inspection checks aimed at verifying compliance with reporting obligations for suspicious transactions and communication with the UIF or the acquisition of specific data and information.

- Issuing risk indicators and disseminating specific models or representative schemes of abnormal behaviors to facilitate the identification of suspicious transactions by obligated entities. Recently, on May 12, 2023, UIF has published a cornerstone new set of risk indicators that will be further analysed in the present dissertation.

The *Anti-Mafia Investigative Directorate (DIA)* [4] and the *Special Currency Police Unit (NSPV)* [5], within their respective competencies, carry out investigative inquiries into the reports of suspicious transactions analyzed and transmitted by the UIF. Conversely, the NSPV and the DIA must, in turn, inform the UIF, also based on specific protocols of understanding, about the investigative outcomes of the scrutiny of suspicious transaction reports, subject to rules regarding investigative secrecy.

[4] https://direzioneinvestigativaantimafia.interno.gov.it/

[5] https://www.gdf.gov.it/

Figure 1.5: Main functions of the UIF

The final but crucial actors in fueling the machinery of anti-money laundering analyses are the *operators* stationed at the gateways of legal circuits and in key positions to intercept potential money laundering and terrorist financing activities. They are called upon to collaborate with authorities by promptly identifying and reporting possible transactions linked to criminal activities.
The scope of obligated entities has expanded over time and therefore specifically identified as "Obliged reporting entities" and now encompasses numerous homogeneous categories of subjects. The initial, traditional group of obligated entities includes banking, financial, and insurance intermediaries, as well as other financial operators. Financial intermediaries, in particular, have the ability to submit a report on a suspicious transaction either "on the ground", for instance, from a branch when they directly observe suspicious activity or actions by one of their clients, or through monitoring centers that oversee the entirety of their clients' transactions and detect anomalies compared to regular flows.
In addition to these, the reporting obligation has been extended to include categories of professionals (notaries, lawyers, certified public accountants, auditors, and audit firms) and non-financial operators (providers of services related to companies and trusts, entities engaged in the trade of antiquities or artworks, or acting as intermediaries in the trade of such works, even when this activity is conducted by art galleries or auction houses, provided that the value of the transaction, even if divided or related transactions, equals or exceeds 10,000 euros; entities that store or trade artworks or act as intermediaries in the trade of such works, provided that this activity takes place within duty-free zones and the value of the transaction, even if divided, or related transactions equals or exceeds 10,000 euros; debt recovery

activities, custody and transportation of cash, securities, valuables, professional gold operators, entities engaged in civil mediation activities, real estate mediation activities, including in the case of intermediaries in the leasing of real estate, limited to operations for which the monthly rent is equal to or exceeds 10,000 euros).
In line with the evolution of the international framework, service providers related to the use of virtual currency and digital wallet service providers have been included among the obligated entities. Specific provisions are also dedicated to gaming service providers (online, physical network, gaming establishments) and gold buyers.
The Public Administration is no longer formally included among the obligated entities; however, certain offices are required to communicate to the UIF data and information concerning suspicious transactions, based on instructions recently issued by the UIF itself.

1.5.1 New risk indicators

On May 12, 2023, the UIF published a provision containing anomaly indicators aimed at banking and financial intermediaries and all obligated entities mentioned above.
There are a total of 34 indicators[6], divided into three main sections and further articulated into a total of 434 sub-indicators. The first section (A) includes indicators from 1 to 8, which highlight profiles identified by framing characteristics of the subject to whom the activity is related. The second section (B) includes indicators from 9 to 32, designed to investigate the sector of activity involved in the transactions. Indicators 33 and 34, belonging to section C, investigate activities that may have a connection with the financing of terrorism or the proliferation of weapons of mass destruction.
The novelty introduced by this provision is the explicit distinction between objective (related to the transaction carried out) and subjective (related to the counterparties of a given transaction) indicators, with the requirement that, for a report sent to the intelligence unit, a specific analysis has to be delivered including evaluation of suspiciousness of both the subjective and objective indicators featuring the transactional anomaly found.

1.6 Intesa Sanpaolo positioning

Intesa Sanpaolo is officially acknowledge in the Bank of Italy as a bank and, as such, is subject to obligations towards the relevant authorities in the field of anti-money

[6]Provision for new risk indicators, 12 May 2023

laundering. These obligations entail that the institution must report suspicious transactions to the UIF (Financial Intelligence Unit) in the event of any irregularities in the activities of its clients.
In the Intesa Sanpaolo internal organisational structure, the AML activities are grouped in the Compliance Governance Area within a specialised Central Directorate, namely Anti Financial Crime Central Directorate, that acts as a pivotal unit in charge of the overall AML/CFT activities in the Intesa Sanpaolo Group.[13] Considering the Italian market, namely ISP Head Office directly enforces the AML/CFT provisions in the pertinent Business Units such as Banca dei Territori (BdT), Corporate and Investment Banking (CIB) and the Private banking pole. In this perspective, the transaction monitoring (TXM) and reporting of suspicious activities within Intesa Sanpaolo are structured through multiple processes involving various central organisational units, each responsible for one or more aspects of the overall process.
From another perspective, the mechanism can be viewed through multiple levels on which several processes are structured. For example, transaction monitoring can be considered as a macro process, while the design, calibration, and introduction of algorithms are sub-processes contributing to the overarching process.
It is essential to distinguish between core processes, which align with Intesa Sanpaolo's legal obligations as a financial intermediary, and complementary processes that do not directly pursue the primary objective but are crucial for its performing.
To delve into one of the core processes and contextualize the work discussed in this thesis, it is helpful to outline the path of a suspicious activity report and then focus on the input to this process.

The chain for reporting suspicious transactions within Intesa Sanpaolo consists of four levels. Suspicious transactions, which begin as simple transactions in the first link of the chain, are identified through a targeted screening and filtering process that becomes increasingly refined as it progresses up the chain. At the core of this mechanism lies the Models Analytics and Special Investigations office, known as MAS. Basically MAS provides ISP with the supervision and development of the transaction monitoring systems active in ISP, which takes input from transactions and generates *detections* to spot suspicious activity.
Detections, or first-level *alerts*, are further analyzed by the first-level competent center, which classifies them as "closed as not relevant" in the case of false positives or when they do not show valid reasons for further escalation. If, however, the alert raises sufficient suspicion and necessitates further investigation, the first-level competent center promotes them to *cases* and forwards them to the second-level competent center.
The second-level competent center assesses the adequacy of the analyses conducted at the first level and, through potential integration of additional information, carries

out further analyses or decides to archive the case. If the decision is made to initiate the suspicious activity reporting (SAR) process, the analysis and transmission to the UIF are in the hands of the unit that operates on behalf of the person responsible for reporting suspicious transactions, which is the final link in the chain.

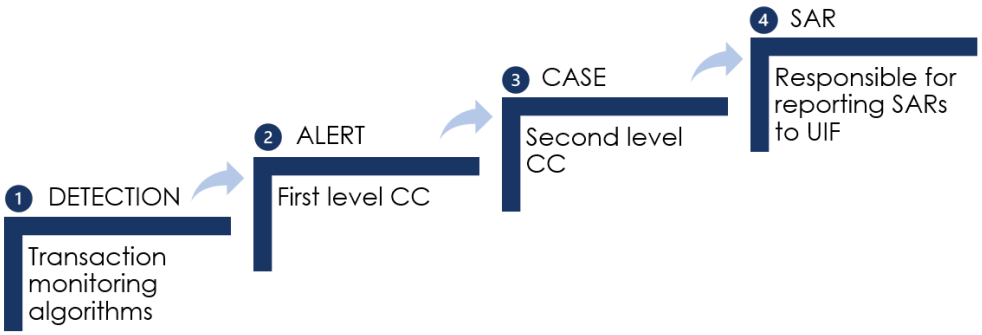

Figure 1.6: Chain for reporting a suspicious transaction: from Detection to SAR

Now, taking a step back to the foundation of this reporting chain and returning to the activities of the office at the base of the chain, the identification of anomalous transactions within datasets containing all client transactions is itself a set of processes supported by transaction monitoring algorithms. These algorithms, whether proprietary to Intesa Sanpaolo or provided by an external vendor-supplied software suite, aim to capture illicit money flows by setting conditions and threshold parameters that seek to incorporate and thus bypass money laundering logic.
The diversity of algorithms can be explained by the intent of those monitoring transactions to identify various forms of criminal activity and to address the diversity of information available.

Chapter 2

Money moving by wire transfers

2.1 How wire transfers work

A wire transfer is a digital method for transferring funds through a network managed by global banks and transfer service agencies. The process involves both a sending and receiving institution and requires specific details from the party initiating the transfer, such as the recipient's name and account number [14]. Unlike physical cash exchanges, wire transfers are settled electronically and can be conducted between banks or through non-bank services. These transactions facilitate the swift and secure movement of money, allowing parties in different geographical locations to transfer funds securely.

Typically initiated by one financial institution to another, wire transfers entail the exchange of information about the recipient, recipient's bank account number, and the transferred amount. The sender, who covers the transaction costs upfront at their bank, provides crucial details such as the recipient's personal information, banking specifics, receiving bank's information, and the purpose of the transfer. Once the necessary information is recorded, the wire transfer begins. The initiating firm dispatches payment instructions to the recipient's institution via a secure system. Upon receiving this information, the recipient's bank deposits its reserve funds into the designated account, and the two institutions settle the payment on the backend after the money has been deposited.

A payment system or clearing and settlement system encompasses three fundamental components:

1. Clearing System: involves the reconciliation and netting of transactions before the actual settlement of funds can occur.

2. Settlement System: encompasses multilateral arrangements and systems designed for the clearing, settlement, and recording of various financial transactions, including payments, securities, and derivatives.
   There are different types of settlement systems, including:

   - Net Settlement System: Involves the netting of payment obligations among participants, reducing the overall settlement amount.
   - Real-Time Gross Settlement System (RTGS): Provides for the immediate and individual settlement of transactions, without netting, enhancing efficiency and reducing risk.
   - Real-Time Final Settlement System: Similar to RTGS, this system ensures final and irrevocable settlement in real-time.

3. Messaging: plays a crucial role in facilitating communication between banks and the Clearing and Settlement System (CSM). It serves as the means for transmitting information related to transactions, ensuring coordination and information exchange between participants in the payment system.

These elements collectively contribute to the smooth functioning of payment systems, ensuring the accurate and timely processing of financial transactions.

2.1.1 Centralized message, clearing and settlement system

Each bank having a direct contact with any other bank in terms of clearing and settlement implies a relevant amount of complexity and inefficiency. This is the reason why countries located in the same area/economic area are grouped under a centralized clearing and settlement system operating under central banks (Figure 2.1).

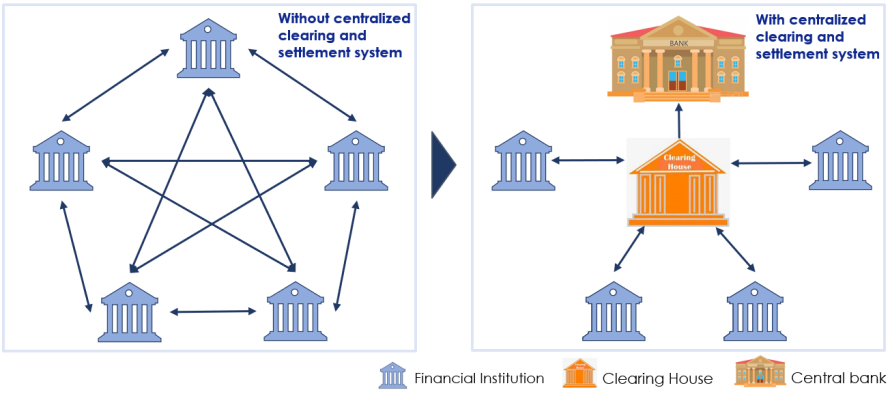

Figure 2.1: Different wire transfer schemas

In modern economies, the distinction between large-value payment systems and retail payment systems is based on the nature of payments [15]. Large-value payment systems are involved in interbank transactions, such as money market contracts, foreign exchange operations, or transactions of significant amounts. On the other hand, the exchange, clearing, and settlement of low-value payment transactions are managed by retail payment systems.
In the Euro area, the retail payment system (so-called "ancillary systems") which handle the exchange, clearing, and settlement of low-value payment transactions (usually equal to or less than 500.000€), operate in an aggregated form with settlement in multiple daily cycles (Net settlement system). This is the case for the type of operation discussed in this work.

The private platform managed by EBA Clearing [16], serving as the Clearing and Settlement Mechanism (CSM) for most SEPA credit transfers, is known as STEP2. This platform receives SEPA payment orders, performs clearances, calculates net positions between banks, and sends settlement requests to TARGET2.
TARGET2, the primary large-value payment system operated by the European Central Bank (ECB) and European central banks, handles, among other things, the settlement requested by STEP2. TARGET2 utilizes the Real-Time Gross Settlement (RTGS) system, meaning transactions are processed immediately and individually without waiting for cumulative net settlement.

Information exchange occurs through a messaging system containing all the necessary details. SEPA utilizes its messaging system, which adheres to the ISO 20022 standard which will be discussed later (2.2.1).

In contrast to centralized message, clearing and settlement systems that operate within specific jurisdictional clusters, requiring correspondent banking relationships

(Chapter 3), which operate in case of Financial Institution under different clusters of jurisdiction.

2.2 SWIFT

As a preamble to Chapter 3 and as an alternative to the integrated messaging systems of centralized clearing and settlement systems, there is the SWIFT messaging system (Society for Worldwide Interbank Financial Telecommunication). SWIFT is a centralized and standardized messaging system used in global wire transfer payments, connecting different jurisdictional clusters worldwide (EU, USA, Africa, Asia). It solely manages the flow of orders and receipts in the form of messages sent over its network. A SWIFT message has a standardized format with numbered fields, each designated to contain specific information. The message's name ("MT nnn", where "n" is replaced by numbers) already incorporates information, indicating the category, group, and specific type of the message (2.2).

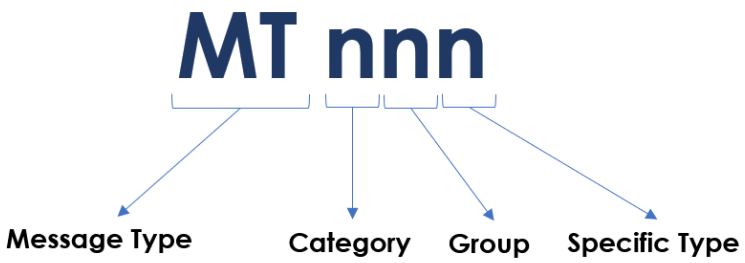

Figure 2.2: MT message

The categories are a total of 10 and are listed in Table 2.3.

Category	Message type	Description	Number of message types
0	MT0*xx*	System messages	-
1	MT1*xx*	Customer payments and cheques	19
2	MT2*xx*	Financial institution transfers	18
3	MT3*xx*	Treasury markets	27
4	MT4*xx*	Collection and cash letters	17
5	MT5*xx*	Securities Markets	60
6	MT6*xx*	Treasury markets – metals and syndications	22
7	MT7*xx*	Documentary credits and guarantees	29
8	MT8*xx*	Traveller's cheques	11
9	MT9*xx*	Cash management and customer status	21

Figure 2.3: MT categories

In Figure 2.4, you can observe an example of a SWIFT message. The message is divided into a "Message Header" and a "Message Text." In the Message Header, circled in red, the message type is MT 103, belonging to the category of Customer payments. There are also details about the ordering customer and the beneficiary, along with transaction identification codes.
In the Message Text, there are various numbered fields filled with corresponding information (highlighted in blue), including details about the ordering bank, information about the receiving bank, and so forth.

2.2.1 New regulatory expectation: from MT to MX format

As the banking landscape undergoes rapid transformation, the introduction of new payment methods necessitates the adoption of a common, modern standard with global applicability. The migration to ISO 20022 began in March 2023, following a roadmap spanning approximately two years. ISO 20022 aims to:

- Improve communication: The XML format of messages is foundational, making communication more standardized and accessible.
- Data-rich messages: The format allows for more comprehensive information within a single message, reducing payment failures and supporting activities such as mining, regulatory reporting, and AML checks. ISO 20022 introduces new roles, such as the Ultimate Debtor and the Ultimate Creditor.
- Multilingual support: ISO 20022 supports multiple languages beyond English, including Chinese, Japanese, Arabic, etc.
- Global adoption: Over 70 markets are actively working on migration strategies and plans, emphasizing the global relevance of ISO 20022.

ISO 20022 serves as an open global standard for financial information, offering consistent, rich, and structured data applicable to various financial transactions. The MX message name is also significant in indicating its typology and incorporates information, as illustrated in Figure 2.5.

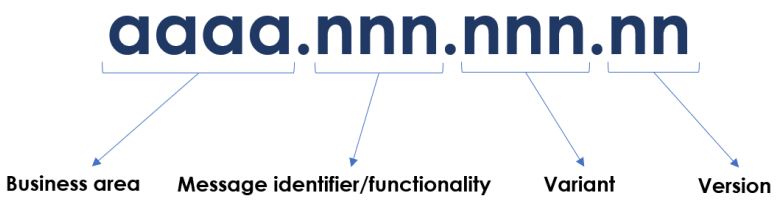

Figure 2.5: MX message

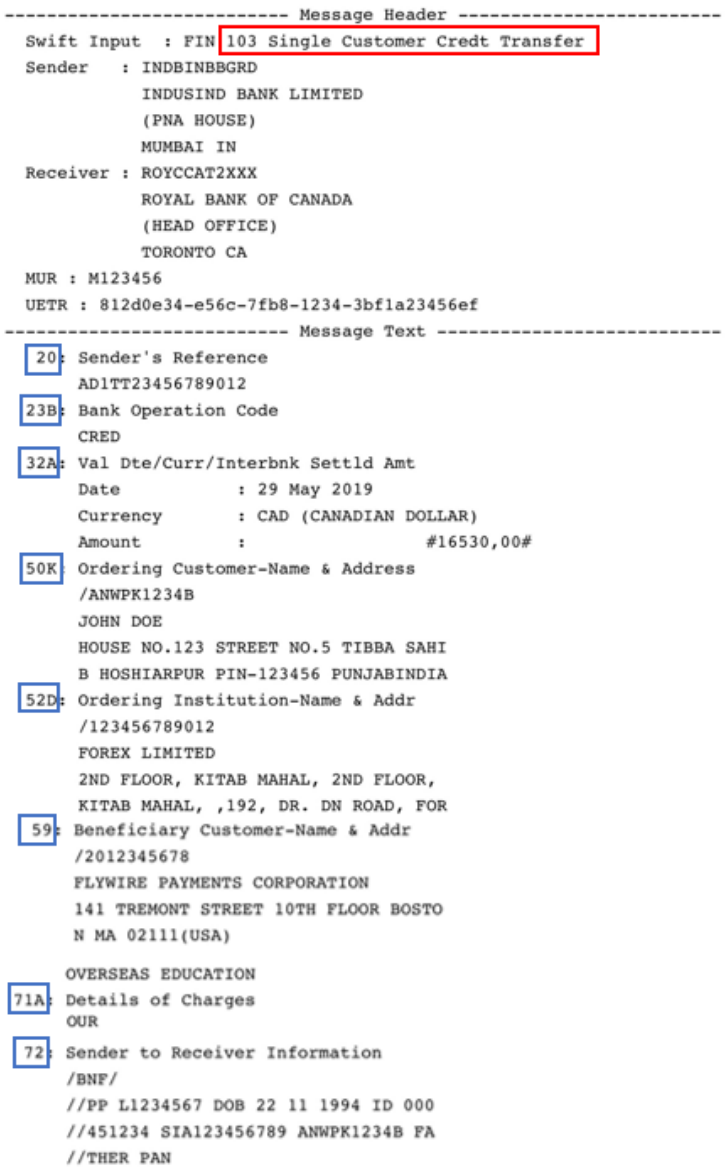

Figure 2.4: Example of an MT message

In Figure 2.6, an illustrative example is provided, depicting a mapping between MT and MX fields.

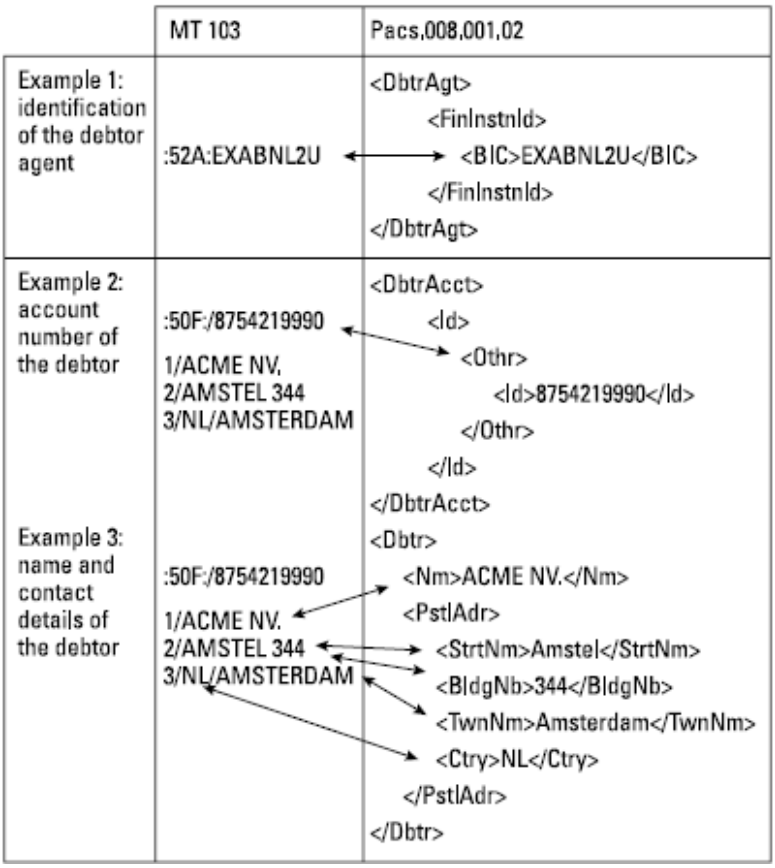

Figure 2.6: Mapping an MT103 to an ISO 20022 Credit Transfer

Chapter 3

Focus on correspondent banking

The primary scope in which payment messages systems (foremost the world-wide SWIFT system) is utilized revolves around the framework defined by correspondent relationships, which, as their core business, encompass cross-border transfers.
The following sections will delve into this activity, elucidating its operation, structures, operational mechanisms, and key international AML/CFT guidelines.

3.1 Introduction to correspondent banking

As a technical introduction to correspondent banking it is worth claryfing the concept of some key concepts that are functional to the development of the following chapters of the present dissertation.

Correspondent banking is “the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank)”. This is the definition given by the FATF ([7]), which is the international organization setting standards that aim to prevent illegal activities and the harm they cause to society.
A more detailed definition is provided by the Bank for International Settlements (BIS) [17], an international organization headquartered in Basel, Switzerland, dedicated to fostering cooperation among central banks. It acts as: "correspondent banking is the provision of a current or other liability account, and related services, to another financial institution, including affiliates, used for the execution of third-party payments and trade finance, as well as its own cash clearing, liquidity management and short-term borrowing or investment needs in a particular currency".

Correspondent banking is a trust-based relationship between two financial institutions that do not operate under the same centralized clearing and settlement systems. Its primary purpose is to facilitate the exchange of funds, serving as a critical component of the global payment system, particularly for cross-border transactions, and a robust mechanism to support international trade. In a correspondent banking relationship, two financial institutions are engaged. This arrangement is established to enable trade between countries operating under distinct jurisdictions. The entities involved in this relationship are named, as previously said, correspondent institution and respondent institution.
While a correspondent banking relationship can involve both banks and Money or Value Transfer Services (MVTS), for the sake of simplicity, we will focus on banks, as the scope is limited to operations related to wire transfers.

The *correspondent institution* is the bank that provides services on behalf of another financial institution. Generally, it does not engage directly with the customers of the other institution, except in cases of payable-through-account, which will be explained later in this chapter.
On the other hand, the *respondent institution* is the one that seeks services it cannot offer directly to its own customers. These customers can be individuals, corporations, or other financial institutions. Services requested through the correspondent banking relationship include, aside from the traditional transfer of funds in local or foreign currency, trade finance-related services, cash clearing, liquidity management, short-term borrowing, foreign exchange, or investments in specific currencies.

There are various reasons why two banks decide to establish a correspondent banking relationship. For example, if a bank in the United Kingdom wishes to process transactions in yen, such as payments to Japanese beneficiaries or yen-denominated transactions, it establishes a correspondent banking relationship with a bank in Japan, which allows it to utilize the services of the Japanese bank. In turn, the Japanese bank can leverage its correspondent banking relationships with banks in other countries to process transactions in foreign currencies, such as euros or dollars, on behalf of its clients. Another example of using a correspondent banking relationship is when a bank in a developing country lacks the resources or expertise to provide a specific service, such as trade finance. In such a case, it can establish a correspondent banking relationship with a larger bank in a developed country that possesses the necessary resources and expertise to provide the required service. This enables the smaller bank to offer its clients access to trade finance services without having to develop those capabilities in-house.

Another crucial concept to clarify is the *nostro/vostro account* [14]. Nostro is

used when describing *my* account held in *your* bank, and this distinction is based on the currency involved. This is distinguishable from the vostro account, which denotes *your* account held in *my* bank and is typically in the local currency. For the sake of simplicity in this paper, we will not differentiate between nostro and vostro accounts; instead, we will consistently refer to them as *loro accounts*. In a correspondent banking relationship, it is possible that just one of the two banks open an account in the other one as well as each of the two banks maintains a loro account in the other bank.

Figure 3 depicts a correspondent banking relationship facilitating fund transfers between two individuals who belong to banks operating in different jurisdictions. Specifically, Bank X, acting as the respondent institution, requests Bank Y, the correspondent institution, to conduct fund transfers on its behalf.
The process begins with funds being debited from customer A, who is a client of Bank X and wishes to transfer funds to customer B. These funds are then credited to a "technical" account held by Bank X. Subsequently, Bank X sends a SWIFT message to Bank Y, requesting the transfer. The funds are debited from the loro account of Bank X, which is held at Bank Y, and are ultimately credited to customer B's account.
The end result is that the funds are transferred from customer A's account to customer B's account, with intermediate balances occurring within Bank X's accounts.

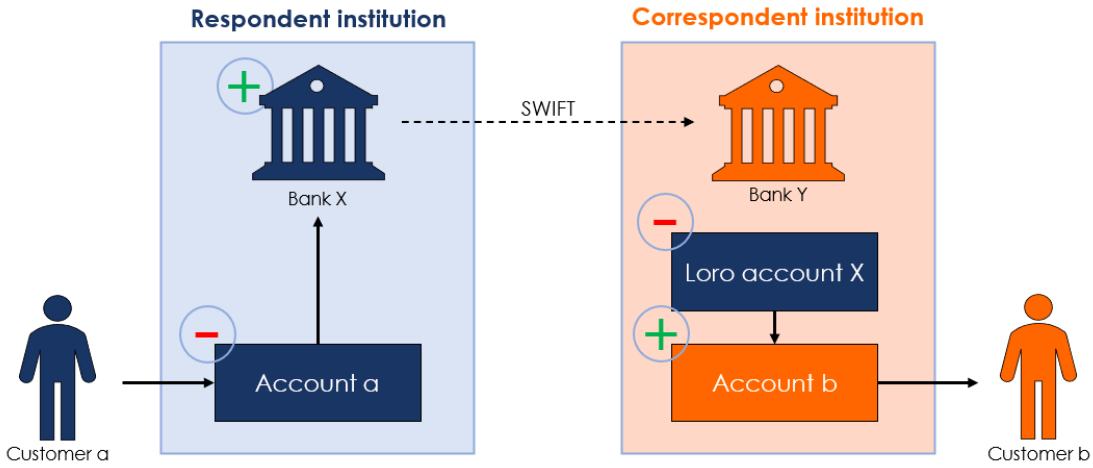

Figure 3.1: Correspondent banking relationship

3.2 Structures of correspondent banking

When it comes to the various types of agreements that can be employed to establish a correspondent banking relationship between two banks, it is possible to identify three primary structures that are globally recognized([18];[19]).

1. In *direct correspondent banking*, the correspondent bank establishes and manages an account for a respondent bank, handling its payment transactions. This arrangement enables the respondent bank to offer services to its customers. However, the customers of the respondent bank do not have direct access to the correspondent banking account.

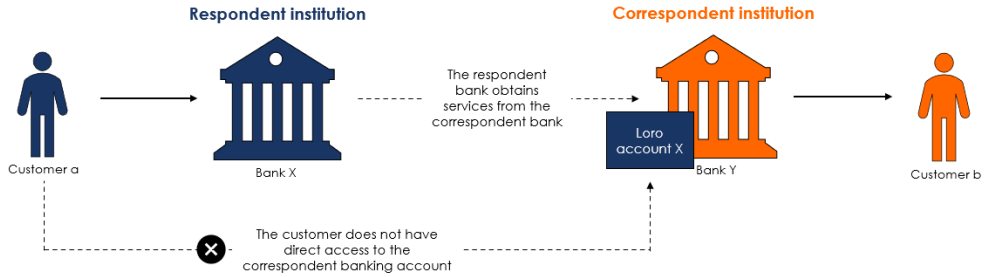

Figure 3.2: Direct correspondent banking

2. In the case of *nested correspondent banking*, a bank's correspondent relationship is utilized by multiple indirect respondent banks, often referred to as nested banks. These nested banks access the correspondent services through their direct respondent bank, which, in turn, holds an account with the ultimate correspondent. Unlike the traditional model, where there is a direct relationship between the respondent bank and the correspondent bank, in nested correspondent banking, an additional intermediary bank facilitates the connection between the nested banks and the correspondent bank.

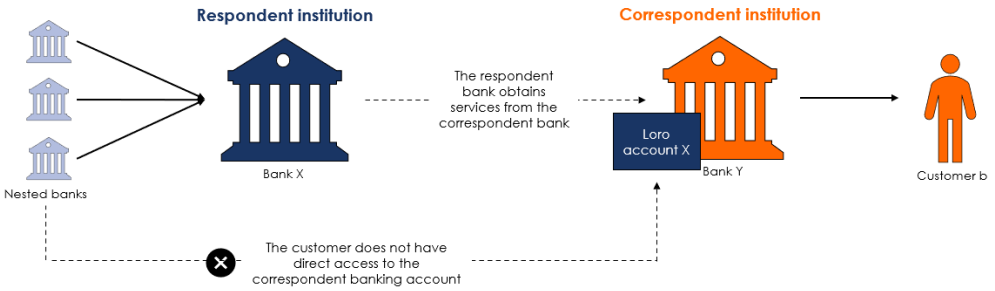

Figure 3.3: Nested correspondent banking

3. In payable-through accounts, the correspondent banking account of the respondent bank is accessible to its customers, enabling them to conduct transactions directly through this account by making deposits and writing checks on the account.

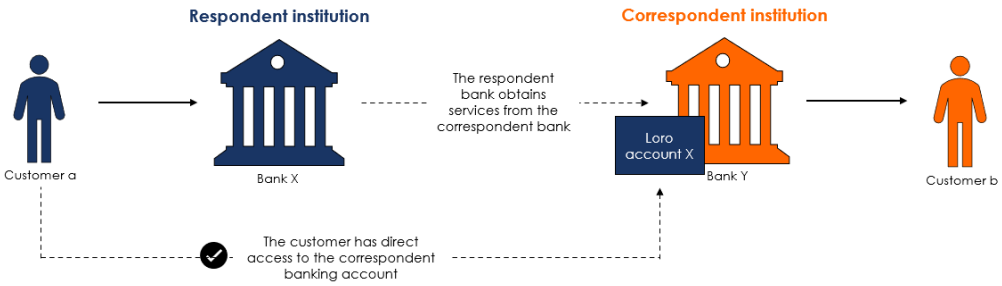

Figure 3.4: Payable-though correspondent banking

3.3 Operating mechanisms

In paragraph 3.2, the three primary agreement types between the respondent and correspondent banks for facilitating fund transfers from customer A to customer B are outlined.
In reality, customer B is not always an individual; instead, the beneficiary of the correspondent institution can be another financial institution. For instance, consider a small European bank that is not part of the SEPA circuit and needs to execute a SEPA wire transfer. This minor bank will rely on another bank with which it maintains an ongoing correspondent banking relationship, and that bank, acting as the correspondent bank, will execute the SEPA wire transfer to the ultimate recipient bank (see Figure 3.5).

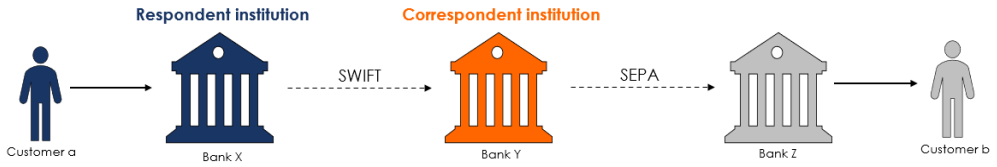

Figure 3.5: Transmission of the SEPA service

More in general, when a bank wants to reach another bank and does not exist any link between those two banks (so they do not accede the same centralized clearing and settlement system and they are not in a correspondent banking relationship), the bank asks one of its correspondent banks to perform the transfer.

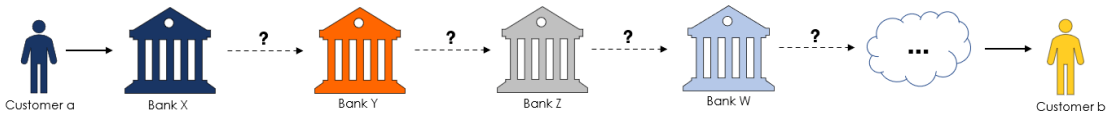

Figure 3.6: Fund transfer involving a series of financial institutions

With reference to Figure 3.6, it is crucial to emphasize that Bank X is unaware of how Bank Y guarantees the service (including the payment systems it uses and the banks it may rely on). Bank X only knows that Bank Y provides the service at a specified cost. Therefore, Bank X is aware of the payer (who is its customer), knows the beneficiary and their respective bank, and is aware that they will approach Bank Y. Bank Y, in turn, can either execute the payment or have a separate agreement in place with another bank, Bank Z, to which it turns. Bank Y is aware of the payer and the beneficiary (and their respective banks) and knows that they will approach Bank Z. Bank Z is informed about the payer and the beneficiary (and its respective banks), Bank Y, and whether they will turn to another bank, Bank W, in the chain. This process continues, and only the last bank, the one directly performing the service, is aware of the entire transaction path (in addition to the beneficiary's bank). The other banks in the chain are only aware of the route from the beginning to the step immediately following their own, in addition to the ultimate recipient. Each step is determined by individual agreements: the transmitting bank establishes an agreement with the correspondent bank because it offered a better price or service than another, but it is unaware of how the service will be guaranteed. Consequently, complex sequences in the flow of funds in correspondent banking can occur at times.
This phenomenon is commonly referred to as *correspondent banking chains*, as illustrated in Figure 3.7, where each bank involved in the chain acts as a "wire-transfers intermediary." Intermediation occurs when a bank facilitates a wire transfer involving another bank. In such transactions, at least one of the two counterparties is not a customer of the same bank.

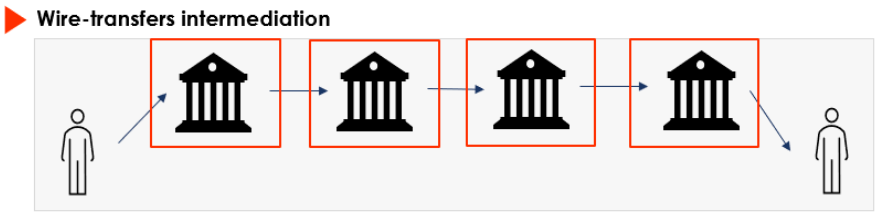

Figure 3.7: Wire transfer intermediation

Depending on a financial institution's position within a correspondent banking chain, it is customary to differentiate between cases where interactions take place

between two banks or between a bank and a customer. With reference to Figure 3.8, we can distinguish between *pass-through* and *direct execution*.
Pass-through, also known as "order prosecution" in some technical jargons, occurs when a bank acts as a bridge between two other banks. In this scenario, neither the originator nor the beneficiary is a customer of the bridging bank.
The direct execution (either beneficiary and ordering case) occurs when a bank performs a wire transfer between one bank and a customer. Considering the originator and the beneficiary, one of them is a customer of the bank that operates.

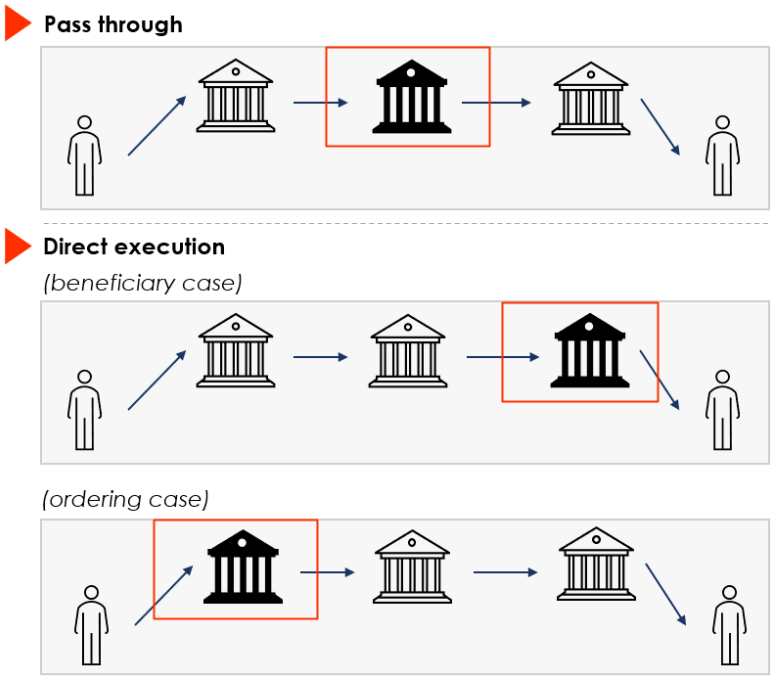

Figure 3.8: Pass through and direct execution

Due to the different set of information available in each case, a given bank in the wire-transfer supply chain may be exposed to different typologies and severity of AML Risks that, in principle, are increased when different players are involved in the operation performing.

3.4 International guidelines on correspondent banking

Engaging in correspondent banking relationships often exposes institutions to cross-border activities. In accordance with the guidelines set forth by major supranational

organisations, the activity of correspondent banking monitoring necessitates additional AML/CFT measures compared to standard monitoring. This is primarily due to the significant disparities in the AML/CFT rules between countries in different jurisdiction as well as information asymmetries occuring in long-range transfer of funds.
Specifically, two FATF recommendations directly address this issue: Recommendation 10 and Recommendation 13 (as previously discussed in Chapter 1.3), both falling under the section titled "Preventive measures".

Recommendation 10, titled *customer due diligence*, outlines the measures to be taken in situations such as establishing a business relationship or conducting occasional transactions. These measures are legally mandated in every country and primarily involve gathering information about the counterparty and the transaction's context to assess AML/CFT compliance. The interpretative note of this recommendation specifies that enhanced controls are required in specific circumstances, particularly those involving multiple jurisdictions.
Correspondent banking relationships, which involve counterparties in different geographic locations subject to different legal frameworks, therefore require what is known as *enhanced due diligence*. This enhanced due diligence encompasses:

- Gathering supplementary information about the customer, the nature of the business relationship, the source of funds, and the purpose of transaction;
- Securing the endorsement of senior management to initiate or maintain the business relationship;
- Conducting intensified monitoring of the business relationship;
- Mandating that the initial payment is executed through an account in the customer's name with a bank subject to comparable Customer Due Diligence (CDD) procedures.

Recommendation 13, on the other hand, is specifically dedicated to correspondent banking. In this context, financial institutions are urged to perform customer due diligence beyond what is required for individual transactions. Specifically, the recommendation encourages:

- Acquiring an adequate amount of information about a respondent institution;
- Evaluating the AML/CFT controls implemented by the respondent institution;
- Securing approval from senior management prior to establishing new correspondent relationships;

- Clearly comprehend the specific responsibilities of each institution;
- Ensuring that, concerning "payable-through accounts", the respondent bank has conducted Customer Due Diligence (CDD) on customers with direct access to the accounts of the correspondent bank.

Based on these recommendations, FATF published a guidance on correspondent banking services in 2016 to clarify its position regarding correspondent banking relationships [19]. The primary reason for dedicating a comprehensive guide to this type of relationship was to address the phenomenon of *de-risking*. This phenomenon is characterized by the avoidance, rather than appropriate regulation, by many financial institutions of establishing cross-border correspondent relationships. This occurs for a variety of reasons, including issues related to profitability, increased compliance costs, and the confusion caused by the term "Know Your Customer's Customer" (KYCC), which does not require conducting Customer Due Diligence (CDD) on the customers of the respondent bank's customers but rather demands that the correspondent institutions knows how CDD is conducted on the respondent institution's customers.

On the possible causes which lead to de-risking, FATF itself published the results of a survey conducted in 2021 [20], revealing the primary factors hindering cross-border payments. As outlined in 3.9, the significant increase in costs associated with implementing more technologically advanced AML/CFT systems is the leading disincentive. Other factors include diminishing velocity, limiting access, and reducing transparency.

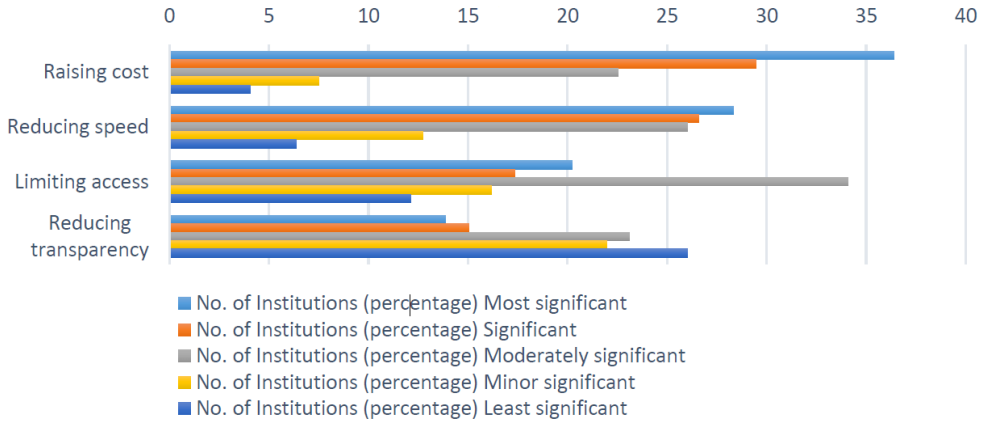

Figure 3.9: Contribution of divergent AML/CFT requirements to challenges

Another comprehensive study that explicitly investigates the de-risking phenomenon was conducted by the Bank for International Settlements (BIS)[21]. This

study utilized data provided by SWIFT from 2011 to 2015, including message types MT 103 and MT 102, which contain information on sent and received volumes and nominal values for each country pair. The nominal values were converted to US dollars using daily exchange rates. The dataset encompasses over 200 countries and territories, categorized by continents and regions.
Given that SWIFT is the most widely used standard for cross-border payments, the data presumably capture a significant portion of correspondent banking activity.

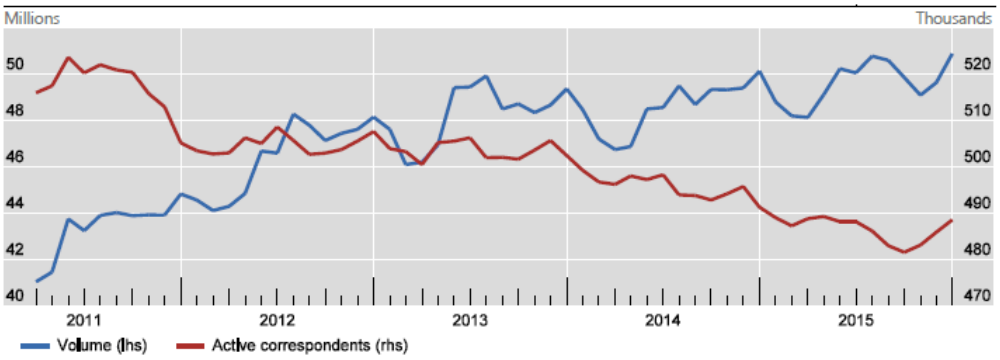

Figure 3.10: Number of active correspondent entities vs total volumes (three-month moving averages is represented)

As evident from Graph 3.10, the overall transaction volumes increased from 2011 to 2015. This might suggest the possibility of an increase in the number of correspondent banks. However, the declining number of active correspondent institutions indicates that the only factor on the rise is concentration. This serves as confirmation of the de-risking phenomenon in correspondent banking, as payments are likely being redirected to other channels after account closures.

Through its guidance on correspondent banking services [19], FATF emphasizes that these relationships are vital for enhancing international trade and by no means intends to discourage the establishment of connections between countries. The aspect it strives to underscore and clarify is that such relationships, involving countries with potentially different legislations, require more in-depth scrutiny and investigations.
Factors to consider when assessing correspondent banking risks may include the jurisdiction of the respondent institution, the products/services it offers, and its customer base. It is not possible to develop an exhaustive list of higher-risk relationships due to various factors, such as the absence of a comprehensive list of risk factors or that both relevant risk factors and applicable risk mitigation measures must be considered together to form an accurate and comprehensive assessment of the risks.

Nevertheless, FATF does list some of the principal activities for entering into a business relationship. The correspondent institution should:

- Verify and identify the respondent institution;
- Understand the ownership and control structure of the respondent institution;
- Gather information to comprehend the purpose and intended nature of the relationship;
- Collect information from publicly available sources regarding the reputation of the respondent institution in terms of being subject to money laundering (ML)/terrorism financing (TF) investigations or regulatory actions;
- Assess the respondent institution's AML/CFT controls;
- Understand how the respondent institution will provide services available through the correspondent banking relationship (assess the structure established, as one of the three discussed in Section 3.2).

Once the risk is identified, and all the gathered information is verified, the next step is risk management.
For this purpose, FATF recommends activities such as ongoing due diligence, which can be conducted at the beginning of the relationship and throughout its duration. Ongoing transaction monitoring is essential, taking into consideration the past behavior of the respondent bank. Targeted monitoring may be necessary, depending on unique factors. Request for Information (RFI) is a critical tool when a transaction is flagged as suspicious. RFI, in particular, involves a request from the correspondent institution to the respondent for more information regarding the transaction. This may include details such as the duration of the relationship between the counterparty and the respondent bank, information on the respondent bank's counterparty, or any possible affiliations of the customer with third parties.

To enhance risk management from the beginning, correspondent institutions can establish a formal written agreement with the respondent institution before providing correspondent services. This agreement should incorporate forward-looking clauses. The agreement's content should address how the correspondent institution will monitor the relationship, the effectiveness of the respondent institution in applying Customer Due Diligence (CDD) measures to its customers, and the implementation of Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) controls.
Furthermore, maintaining an ongoing dialogue with the respondent institution throughout the relationship is crucial.

3.4.1 The Wolfsberg questionnaire

The Wolfsberg Group, consisting of 12 global banks from the private sector, plays a significant role in the management of financial crime risks and offers valuable guidance. Within correspondent banking, the Wolfsberg Group [22] facilitates the establishment of relationships through the release of the *correspondent banking Due Diligence Questionnaire* (CBDDQ). This questionnaire sets a higher standard for cross-border and higher-risk correspondent banking due diligence, while also minimizing the need for additional data, aligning with current FATF guidance. [23] By reducing the demand for extra data, the CBDDQ can contribute to cost savings in compliance and expedite the onboarding process. This benefits both correspondent and respondent banks, and widespread adoption of the CBDDQ enhances overall industry standards, fortifies the international financial system, and helps mitigate de-risking.
The questionnaire comprises 132 questions categorized into 14 themes, which include entity and ownership, products and services, AML/CFT and sanctions programs, anti-bribery and corruption, AML/CFT and sanctions policies and procedures, risk assessments, KYC, CDD and EDD, monitoring and reporting, payment transparency, sanctions, training and education, quality assurance, compliance testing, audit, and fraud.

The CBDDQ, that basically set a "de facto standard" for a document acting as a passport in correspondent banking onboarding process among banks, has been recently update (10/02/2023).
One of the finest changes of the the current version is the enhancement of the questionnaire section devoted to transaction monitoring information.
In this section, for the first time, is introduced the explicit option that a bank may adopt, as a transaction monitoring system for its correspondent banking flows, a vendor-supplied system or an internally-developed one.
This detail testify that since the "on the shelf" market solutions have known improvement areas, many banks are resolving those issues by implementing taylor-made internal solutions expected to be much more performant.
As it will be widely shown in the upcoming chapters, Intesa Sanpaolo has embraced this trend by exploiting its internal capabilities of the already introduced MAS unit.

Chapter 4

Transaction monitoring systems: the current approach and its weaknesses

As mentioned in the preceding chapters, the structure of Anti Money Laundering does not have a single way to be implemented. Instead, it is up to each financial intermediary/obligated entity to decide what internal framework to adopt and how to organize their resources to comply with the national regulatory framework and, more broadly, with the standard issued by FATF[1].

More specifically, the process to be further examined and analyzed is limited to one of the activities within AML/CFT, although one of the most substantial, which is transaction monitoring.
Transaction monitoring, as the name suggests, involves the continuous scrutiny of the countless transactions carried out by clients. In the case of ISP Head Office, the largest core bank in the Italian market, this is about the oversight of a traffic flow of approximately 270 millions transactions per month of which just a very small fraction is suspicious leading to the classic "needle in the haystack" problem. To give an order of magnitude, approximately less than 0,05% of customers are potentially involved in SARs. It's the very nature of seeking something minuscule within a bunch more of legitimate transactions that makes this challenge quite complex. This is compounded by the fact that those engaged in illicit activities aim to remain inconspicuous among the other transactions, employing tactics to obscure and blend their movements with the rest of the transactions.

For obliged entities involved in the activity transaction monitoring, this translates

[1]Decree Law 231/2007

into the need to search for or discern criteria and conditions that allow them to distinguish the behaviors of individuals attempting to exploit financial systems for money laundering or terrorism financing from those who are operating in compliance with the law. What makes this task particularly challenging is that, often, illegal trafficking patterns are distinguishable from legal ones only by subtle, nearly imperceptible nuances.

The following paragraphs are primarily dedicated to illustrating how Intesa Sanpaolo fulfills its obligations, namely the approach adopted in the field of transaction monitoring[24]. Subsequently, with reference to national-level data published by several of the main Financial Intelligence Unit worldwide as well as from public reports coming from strategic consulting companies and accounting firms, the weaknesses of the current monitoring system are highlighted.

4.1 Current transaction monitoring system

In practical terms, monitoring transactions means analyzing the data associated with the movements of a financial institution customer base, using either in-house or external technologies, which consist of monitoring algorithms aiming to detect anomalous activity that may arise suspicious due to its distance from expected customer behaviour. For example, a transaction might be deemed suspicious if the transferred amount is very high and involves a geography known for being a tax haven or a high-risk country. Additionally, the lack of apparent economic purpose or the roundness of the amount could also serve as clues that the transaction is not properly linked with a real underlying business.

In order to spot suspicous activities, the unit of analysis of a transaction monitoring algorithm may be focused on an individual transaction if the condition it incorporates pertains to specific attributes of that single transaction. Alternatively, it can be on groups of transactions when the granularity of the condition to be investigated is identifiable by grouping multiple transactions together. An example will be helpful to better illustrate what has been discussed so far.

Let's assume we are facing an illicit terrorism financing transaction perpetrated by a cross-border wire transfer from a European Country to a High Risk Geography. By human judgment, it's easy to consider, that the counterparty's place of residence could be an indicator of suspicion. In fact, according to a number of different risk indicators issued by Competent Authorities on global scale, if the counterparty's residence with whom the customer is conducting fund transfer belongs to a country categorized as a *High Risk Geography*, further investigation would be advisable.
The fact that a transaction involves one of the parties from a high-risk country is

a characteristic that pertains to the individual transaction and is an extractable data point from a single transaction record.

A different scenario arises when dealing with a money launderer who channels its funds to disperse them among a set of counterparties by dividing the amount. Money launderers often move large sums of money, and it can happen that when conducting a monitoring focusing on individual transactions, the amount within each transaction is not enough to raise any suspicion, as it may be limited (or at least below the algorithm-filtered thresholds). However, if we were to change the granularity of the monitoring and aggregate the transactions on the counterparty who has dispersed that money, we would discover that the cumulative amount is one that requires further investigation.

These two simple and intuitive examples, as well as the numerous other algorithms that handle the millions of daily transactions, are built based on what are known as *risk indicators*. As mentioned in Section 1.2, the Financial Intelligence Units or Competent Authorities (according to national AML system configuration) periodically issue indicators meant to serve as a guide for obligated entities in fulfilling their AML/CFT duties. Moreover, other national and supranational bodies consistently issue guidelines to direct financial operators in their research efforts, which can aim to integrate every piece of information to enhance their monitoring systems. Therefore, the effort that every financial intermediary undertakes to establish a transaction monitoring system should be made with the goal of covering the risks to which they may be exposed, as listed by the indicators pertinent to the business they carry out.

As the risk indicators published over the past 10 years number in the thousands and often exhibit overlap, it is both feasible and beneficial to cluster them into eight macro classes, also referred to as *Red Flag Themes*, which are listed in Table 4.1.

N°	Red Flag Theme	Description
1	Funneling	Funnelling represents the activity of multiple accounts that feed a single account ('many-to-one' activity). This type of activity can represent the money laundering stratification phase and tends to hide the origin and the actual amount of funds.
2	High Risk Geography	High Risk Geographies may be more vulnerable or have been historically abused by money launderers and criminals. Such locations may also encounter strategic weaknesses in anti money laundering and counter-terrorist financing measures.
3	Identity concealment	This category includes a number of ways to hide the identity, of the parties involved in a transaction.
4	Lack of economic purpose	Lack of economic purpose is a category of Red Flags designed to identify transactions without an apparent economic purpose, such as several transactions on the same day from the same originator to the same beneficiary: this type of activity lacks economic purpose as it could be aggregated into a single bank transfer, thus posing suspicion that they were performed just to conceal the actual intended money flow.
5	Profiling	Financial institutions shall develop transaction profiles of the intended use of products/services by their customers, which can then be compared with the actual use of products/services and the transaction profile, potentially triggering detection on unexpected behaviour.
6	Structuring	Structuring is the practice of conducting financial transactions in order to circumvent the reporting thresholds in a purposely fractioned manner.
7	Third parties (non customers)	This category of Red Flags refers to third parties not customers of the bank. The involvement of third parties in certain transactions can lead to a higher risk due to the lack of information available about such counterparties.
8	Velocity	This category of Red Flags refers to the practice of moving funds immediately after receiving them in similar amounts just to add up confusing transactional layers.

Table 4.1: Red Flag classification and description

Another significant aspect of those algorithms is that they typically focuses on the *customer counterparty* because the indicators and the regulation both address the activity of reporting SARs as a reporting related to a client.

Once encompassed what a monitoring algorithm is, what it is based on, and how it functions, the following paragraphs aim to describe an international banking player typical transaction monitoring framework that, in the following paragraph, will be conceptualised as "Entity of Application" of a given transaction monitoring system development. Specifically the paragraph will outline the sub-processes and levels on which this activity is organized. As such, it is fundamental the initial methodological distinction by classifying a set of activities as portfolio alorithm monitoring and another set of activities as individual algorithm monitoring.[24]

Activities regarding transaction monitoring algorithms portfolio are:

- Transaction monitoring risk assesment
- Coverage analysis
- Impact assessment

The transaction monitoring risk assessment is the activity with the aim of assess risks that Entity of Applications undergo. A deep understanding of the business (which business? how is conducted? who are the customers?) is crucial to develop

safeguards preventing the unintended usage of the entity of applications means in such situations.

Regarding the coverage analysis, the process begins with a systematic compilation of AML/CFT risk indicators. The Red Flags relevant to the business of the Entity of Applications are then identified and matched with the set of potential monitoring algorithms. This procedure is conducted to evaluate the effectiveness of controls in addressing the specific AML/CFT transactional risks associated with the business.

Based on the outcomes of the Coverage Analysis deliverable, a thorough assessment of potential gaps is conducted. These gaps are then addressed using a risk-based approach, taking into account managerial aspects related to risk acceptance, fine-tuning of existing algorithms, development of new algorithms, and the introduction or expansion of manual controls.
Activities regarding single transaction monitoring algorithms are:

- Design
- Calibration
- Refresh
- Decommisioning

Each of these activities is related to each individual algorithm, whether it's internally designed or externally provided. It's important to highlight that the approach used in designing monitoring algorithms is to associate each algorithm with a risk indicator category (Red Flag Theme). The algorithm, therefore, aims to identify specific situations targeted to cover particular scenarios. For example, considering the *velocity* Red Flag Theme, one of the associated algorithm focuses on capturing scenarios where, concerning a customer's current account, a certain amount of money enters and then exits in the same amount in a small time frame.

The algorithm's *design* involves identifying key criteria to frame a specific situation and then translating these criteria into logical conditions that, when appropriately integrated into the algorithm, capture transactions with these characteristics.

Next comes the algorithm *calibration*, which involves fine-tuning the thresholds so that it maintains consistency in terms of relative importance compared to other active algorithms within the overall framework and in proportion to the type of entity it's applied to.

Calibration is the most sensitive phase in the setting of a proper transaction monitoring system since it is crucial to strike the proper balance between detection volume and investigative significance while considering the unavoidable contextual limitations such as the capacity available to evaluate an

Periodically, with the aim of enhancing monitoring quality, the algorithms undergo a *calibration refresh*, meaning a readjustment of the algorithm thresholds.

Finally, if a specific algorithm is no longer deemed effective in detecting anomalies, it can be decommissioned. This phase is also referred to as the *decommissioning* phase.

4.2 Statistics of the actual monitoring system

With the aim of giving a numerical support to the technical illustration of the actual monitoring system, this paragraph aims to report some statistics exposed by the Italian FIU, namely UIF, and published in the semestral report "Statistic data" of I semester 2023.[25]

First of all, the table below shows the comparison between how many SARs were collected versus how many of them were analysed considering the last 5 years. The main fact coming out from this graph is the growth in the number of SARs reported to UIF during the last years.

Another crucial element for an intermediary financial institution in gauging the significance of having an efficient monitoring system is the percentage distribution of those reporting suspicious transactions, categorized by the type of reporting entity.

The graph in Figure 4.2 clearly illustrates the prevalence of banks and post offices compared to other obligated entities in submitting suspicious activity reports (SARs). In fact, out of the 77,693 SARs received by the UIF during the first half of 2023, 41,954 originate from these entities.

Given that this number is quite significant compared to that of other obligated actors, having a system capable of producing targeted SARs, meaning as few as possible with the highest possible accuracy, has a significant impact on the workload of the UIF.

Finally, it is reported the breakdown by means of transfer of the totality of the SARs. This is crucial to understand the importance of having a an accurate

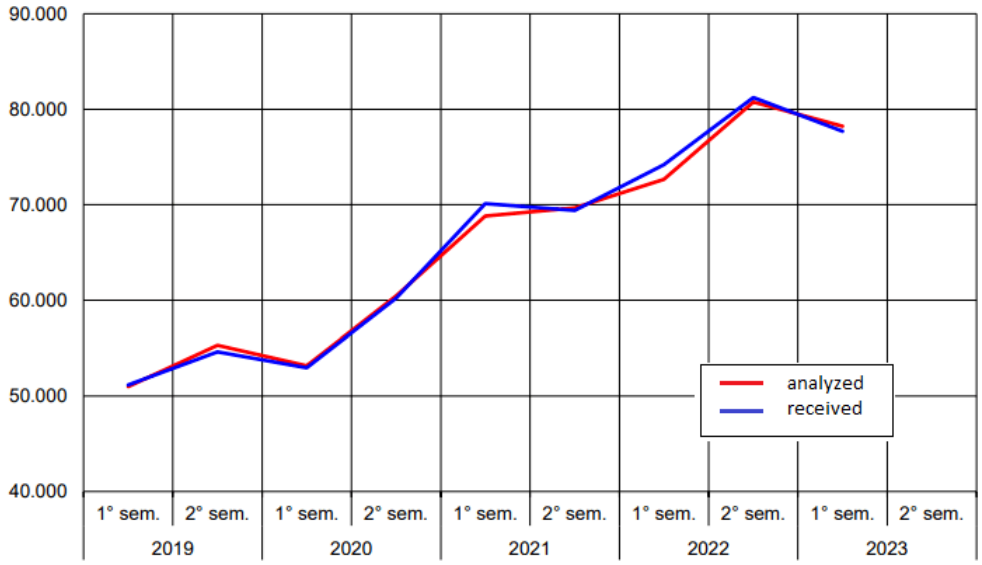

Figure 4.1: Received vs analysed SARs by UIF

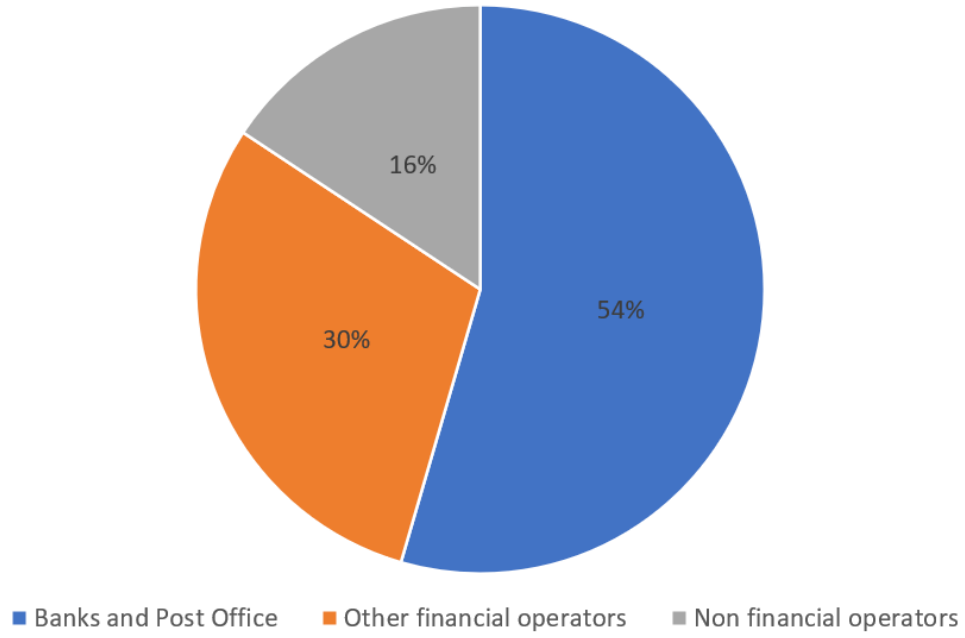

Figure 4.2: Distribution by reporting groups

monitoring system for determined form because relevant considering the totality of the movements.

From Figure 4.3, referring to Banks and Post Offices coloumn, a predominance

TECHNICAL FORM	Banks and Post Offices	Other intermediaries and financial operators	Practitioners	Other non financial subject
National wire transfers	58,3	19,9	0,6	0
Cash operations	10,9	0,9	0,2	0,3
Foreign wire transfers	11,8	11,9	0,3	0
Payment cards and electronic money	9	34,6	0	0,5
Transactions in cashier's cheques	3,1	0,2	0,1	0
Transactions with credit securities	2,5	0,2	0,1	0
Transfer provisions	0,1	31,1	0,6	0,1
Corporate operations	0	0	34,2	0
Real estate operations	0	0	51,1	0
Games and betting	0	0	0	62,5
Trade in gold and precious stones	0	0	0	2,4
Other	4,3	1,1	1,1	34,2
Total	100	100	100	100

Figure 4.3: Breakdown of the main technical forms of payment by type of reporter

of national wire transfers, cash operations and foreign wire transfers comes out. Translated, this means that cash and wires are favorite methods for money launderers to move money. Furthermore, the relevance of foreign wire transfers points out that schemes of illicit traffics go beyond national perimeters and have a wider range of action.

4.3 Functional weaknesses in monitoring Correspondent Banking

Considering large financial institutions, the presence of automated transaction monitoring system, is compulsory due to the volume of transactions and the remote ordering of them by digital means used by customers that make any manual oversight humanly impossibile.

In the Italian landscape, a historical transaction monitoring suite was developed by a joint effort in the private sector with a relevant interaction with competent authorities becoming, de facto, a standard reference for the Italian banking market

and one of the most advanced experience in Europe. Through time, many others systems have appeared in the AML software market that, at their core, share almost the same algorithmic approach.

In most recent times, for sake of both effectiveness and efficiency, major banking players have started to produce in-house solution that are taylor-made for their own business and IT legacy.
Since those experiences are quite a few and pioneristic, it is safe to state that the standard market practice is grounded in the standard features offered by market suite that, so far, present more a plain-level field rather than a relevant differentiation.

In the context of the present dissertation, leveraging the unique experience of the Models, Analytics and Special investigation team of Intesa Sanpaolo in terms of maarket TXM suites in multiple jurisdictions and financial business, such TXM landscape is outlined without specific reference to commercial product.

Wire transfer activity, especially in the cross-border setting and chiefly when performed by complex Correspondent Banking schemas, is a demanding benchmark to assess strenghts and weakness of the current standard transaction monitoring systems.

Correspondent Banking refers to the mechanism mentioned in Section 3, where cross-border fund transfer, especially between two countries not operating under the same message, clearing, and settlement system, and lacking existing correspondent banking relationships, occurs through the intermediation of third parties. This effectively leads to the creation of extended chains involving an originator, a beneficiary, and in general, up to six, intermediary agents.

As extensively highlighted in Section 4.1, commercially available monitoring algorithms operate by grouping transactions at the level of the customer counterparty.
In addition to this, a second characteristic of these algorithms is that, concerning the respective originator or beneficiary, they only conduct checks on the origin or destination of these funds.
In other words, in a chain of correspondent banking, the only checks are on the starting and ending points, and there is complete opacity regarding the intermediary links. However, based on what has been discussed so far, it could very well be plausible that one of the intermediary banks belongs to a High Risk Geography. In such a case, in compliance with FATF standards and current legislation, the transaction should be subject to enhanced scrutiny.[9]

In addition to the lack of transparency regarding intermediary routing, the scope of standard monitoring algorithms is limited to checking the nationality of the ordering or beneficiary bank. This implies that if the bank's nationality does not fall into categories requiring additional scrutiny, regardless of the nationality of the counterparty associated with that bank, the transaction may not necessarily be subject to observation.

In figure 4.4, there is an illustrative use case of a transaction originating from a Russian account held in a Cypriot bank and passing through a Turkish bank before reaching a customer of the financial institution in object. The three countries involved in the transaction have reasons to be subjected to additional scrutiny for different reasons: Russia and Turkey are officially listed as high risk geographies, while Cyprus is well-known for its status as a tax haven and, therefore, a hub for shell companies.

However, the standard algorithms, considering that Cyprus is part of the SEPA network and therefore not viewed as a geography that raises suspicions, and considering that Russia and Turkey fall into the category of high-risk geographies but concerning fields that are not being observed, does not detect any anomalies in the transaction. Consequently, it allows the transaction to proceed without triggering further investigations.

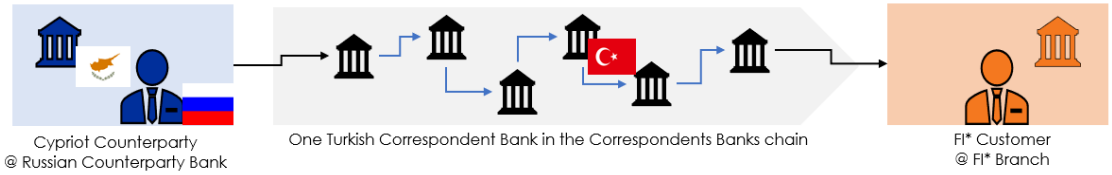

Figure 4.4: CB chain including High Risk Geografy

4.4 Functional weaknesses in detecting schemas with a pivotal player outside customer base

While focusing the transaction monitoring system over the customer base of a given Entity of Application is reasonable from an operational point of view (combining both the core of the SAR obligation as well as the possibility for an Entity to terminate or freeze an account with suspicious activity), even the counterparty side external to the Entity of a given wire transfer may have many insights to tell. As evidence of this, we will now analyze a case related to one of the red flag themes (Table 4.1): the so-called *funneling*.

Funneling is the activity where multiple accounts feed into a single account (which can also be implemented in the opposite direction, with a single account feeding multiple accounts). This type of activity can represent the money laundering stratification phase and is often used to obscure the origin of funds.
In the schema in Figure 4.5, it is assumed that the counterparty intending to feed the other accounts is the customer counterparty of the bank we are using as a reference point. Current monitoring systems aggregate their transactions on this customer counterparty and can easily trace this pattern.

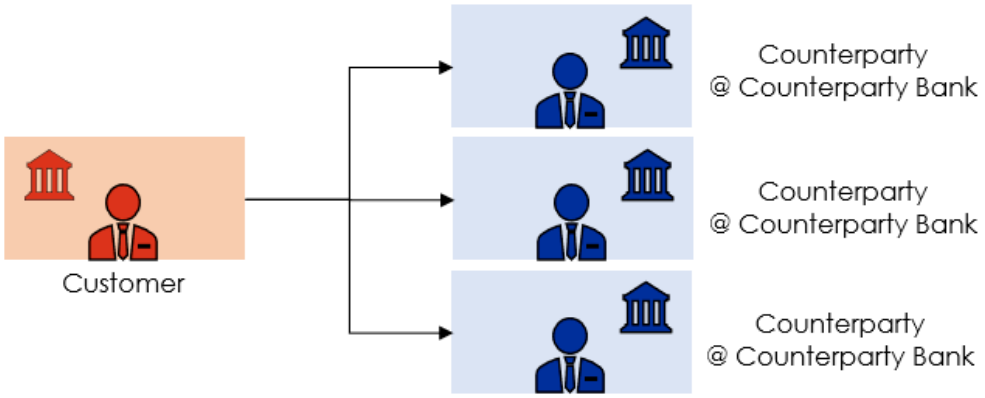

Figure 4.5: Transactions aggregation on a customer

Now, considering the opposite scenario where the account feeding other accounts does not belong to the bank we are using as the point of view (Figure 4.6), it is not guaranteed that monitoring algorithms can detect whether the bank's customers are involved in money laundering activities.
This is because, as the focus is on each individual customer, in the illustrated scenario, each customer's transactions may only reveal simple money movements that don't raise any suspicion, such as not being of an excessively high amount or not involving a counterparty from a High Risk Geography.

This funneling pattern would only be discernible by an algorithm that aggregates on the non-customer counterparty. Only then could one trace the information that many of the bank's customers are linked to a single counterparty. This could be evaluated as a point for further investigation.

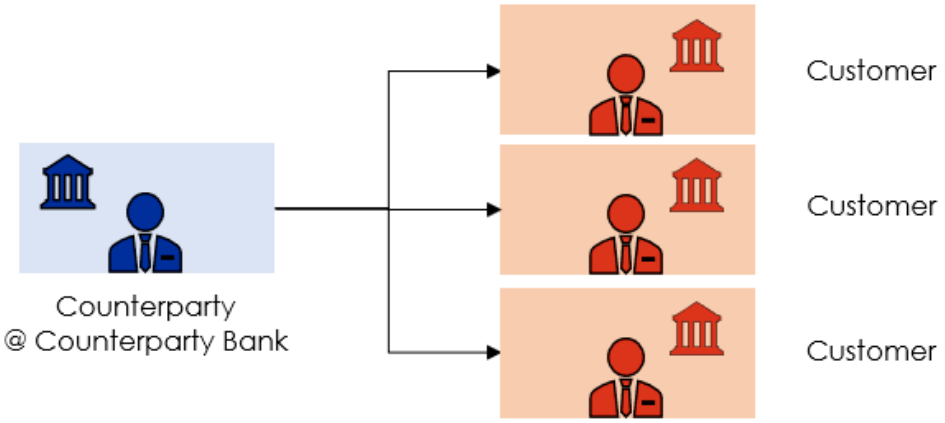

Figure 4.6: Transactions aggregation on a not-customer counterparty

In summary, the focus on the counterparty, which is not currently implemented in the vast majoirty of the commercially available algorithms, is not a search that aims to discover which of your own customers are the core of illegal activities. Instead, it can be a tool that reveals which of your customers are involved in the activities of other entities.
This new insight has a dual effect: on one hand, it helps identify which of your customers are engaging in illicit activities, and on the other hand, in the spirit of collaboration and information sharing promoted by the European Union, it may bring to light money laundering schemes that involve individuals belonging to different financial intermediaries enabling further collaborative investigations.

It is to be reported that the current standard approach reflects the viewpoint of the KYC provisions requiring banks to basically acquire advanced information only on their customers and not on their counterparties. In a nutshell, the core expectation is that a bank is going to monitoring its own customer base and the behaviour of its customers in using the means of payments that the financial institution is supplying to them.
Notwithstanding that this is a clear priority, it is not possible to achieve a comprehensive intelligence of money flows while considering just a single side of the coin.

4.5 Misleading algorithms bringing to false positive

In the context of analyzing the characteristics of the actual approach, another important point to highlight is that the actual mechanism of implementing algorithms, which is one risk indicator to one monitoring algorithm, can sometimes be too basic and can detect schemes which are perfectly legit.

As an example, let's consider the *funneling* Red Flag Theme (Table 4.1). From the definition, it describes a "many-to-one" or "one-to-many" activity.
For simplicity, the analysis is circumscribed to the one-to-many case which is one actor distributing a certain amount of money among several counterparties. In order to capture this behaviour it would seem a good approach building an algorithm that incorporates the same mechanisms and try to isolate the schema. This activity mainly regard wire transfer activity so the perimeter of analysis is delimited to transactions that are wire transfers. The first step for that aim is the aggregation on the originator counterparty as in Figure 4.7 setting temporal range of one month.

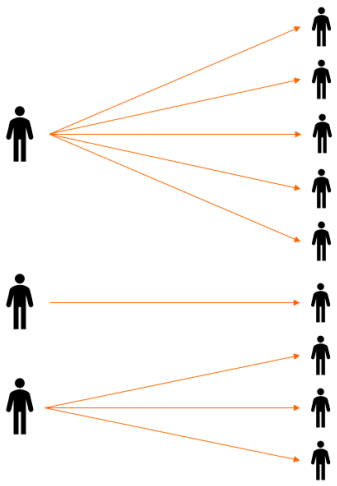

Figure 4.7: Aggregation of transactions by the originator counterparty

Once the counterparties are associated to their outcoming transactions, it is possible to proceed with arguing which selection can be made to isolate the money launderers.
The two parameters on which basing the choice and identifying the launderer profile are:

1. The total amount transmitted in one month

2. The total number of outcoming transactions in one month

About the total amount transmitted, according to human judgment, a sum of at least 10.000€ transmitted in one month can be significant in terms of suspect. For what concern the number of transaction, instead, it could be reasonable a constraint of at least 3 wires performed in one month.
Choosing these thresholds is nothing more than writing the condition of the algorithm that analyzes the transaction. As a result, according to the algorithm, the the outlined profile of a money launderer is one person who transfers at least 10.000€ and at least with 3 different transactions.
As an application of what said until now is the example in Figure 4.8, in which we have to select which from A), B) and C) is suitable for being a possible money launderer, A) will be the only profile selected from the algorithm.
In fact, B) moves 11.000€ per month, which is above the threshold for this metric, but it is not selected as a suspicious case because the number of transaction is under its respective threshold.
The same, even if inverted, happens with case C), in which the threshold of the total number of transactions is exceeded but the amount transmitted is lower than 10.000€.

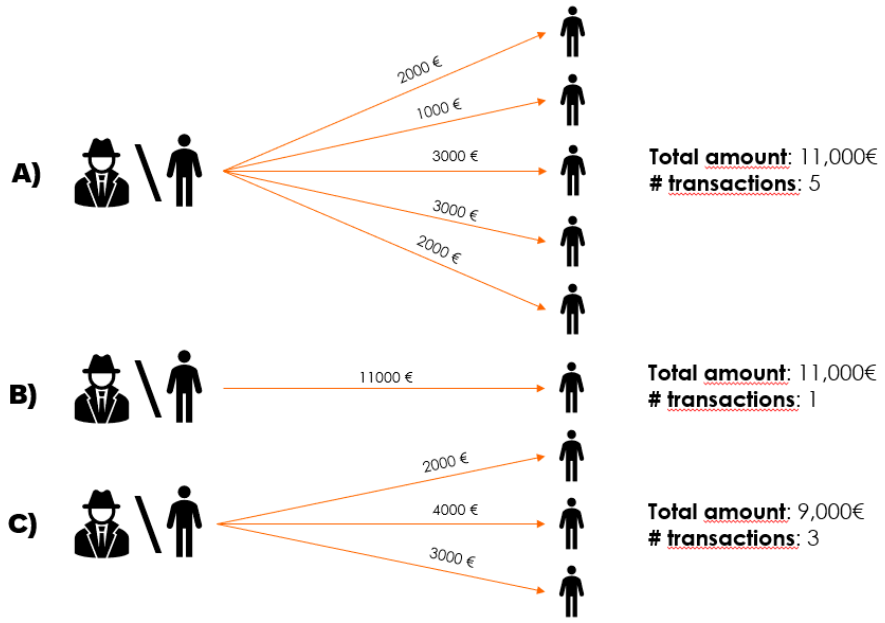

Figure 4.8: Comparing the activity of different subjects

When implementing the search for profiles with these characteristics, one quickly realizes that the result is not as accurate as hoped. In fact, although a monthly total of at least €10,000 transmitted and a number of wire transfers greater than 2 may indeed be plausible for a money launderer, one only needs to consider a small company that pays its employees at the end of the month to observe the same pattern (Figure 4.9).

This means that the algorithm is not sophisticated as much as to distinguish an illicit traffic from a normal operative case and this leads to incur in a lot of false positive cases.

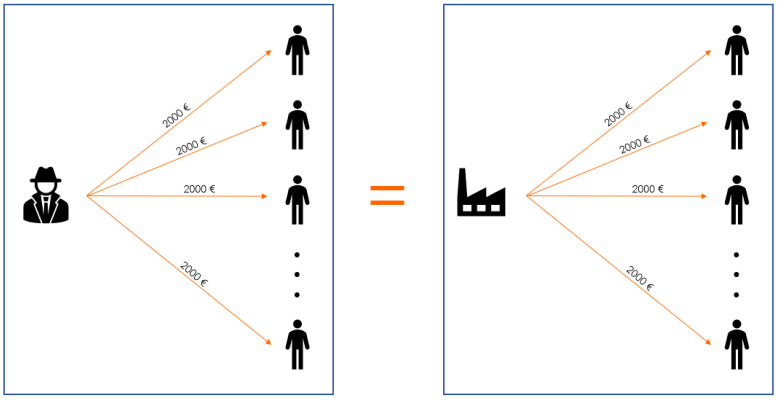

Figure 4.9: Confounding behaviour between a money launderer and a firm paying salaries to its employees

4.6 Macro-implications for the current transaction monitoring

If the preceding paragraphs delved into the technical weaknesses of the standard algorithms adopted by obligated entities, the next one will delve into the consequences at a macro level and, therefore, highlight the shortcomings that afflict the current transaction monitoring system.

The two main effects are:

1. Financial institutions struggling for efficiency: a high number of reporting with a very small accuracy

2. Relentless growth of SARs filing per year sent to UIF

The first observed effect is the high inefficiency of financial institutions in terms of economic effort and workforce when it comes to identifying actual cases of anomalies.
Speaking in terms of numbers, considering data from over 10 international benchmarking exercises conducted from 2018 to 2023 ([26, 27, 28, 29, 30, 31, 32, 33, 34]), it is revealed that large financial players tend to organize their suspicious activity reporting into two subsequent investigation levels, starting from detection disposition to case deepening, leading to SARs filing. Less complex players may adopt different organizational solutions but encounter similar challenges.

Despite a significant range of variability based on size, geographical reach, and business lines, there is an overall average unsatisfactory performance, with 100 detections resulting in only 3 SARs. This percentage is calculated, referring to the graph below, by considering a total of 100% of reports, of which, on average, only 20% is escalated from the first level to the second level. Furthermore, considering that 20% as the new total of anomalous transactions, only about 25% of these are actually promoted to SARs.

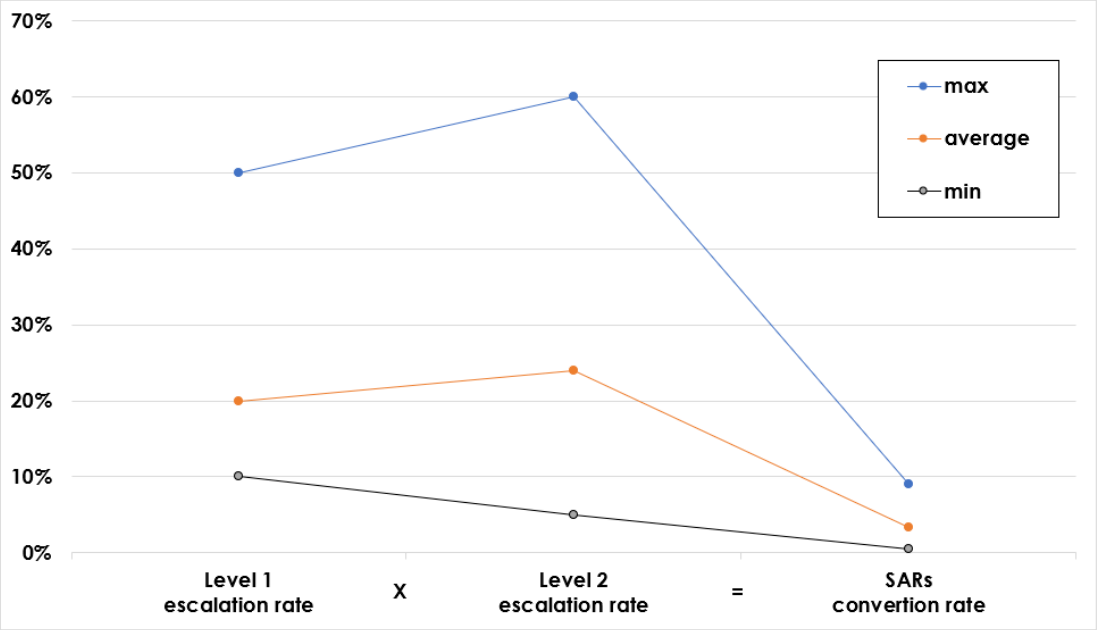

Figure 4.10: Financial Institution struggling for efficiency

Moreover, it is worth mentioning that no significant progress in improving SARs convertion rate is reported in the last 5 years despite the effort engaged in this activity.

The second notable observation in terms of numbers, indicating a problem in the current transaction monitoring system, relates to the congestion of intelligence units. This phenomenon, as evident in Figure 4.11, is not limited to Italian system. While FIUs tasks and regulatory frameworks are challenging to compare, there is overwhelming evidence of a substantial increase in SARs filings from obligated entities being a widespread issue.[35, 36, 37, 38]
Although there are limited public insights on this matter, it is widely reported that only a fraction of SARs provides significant investigative contributions to Law Enforcement Agencies (LEAs). According to Europol, the average proportion of SARs that undergo further investigation at the EU level is approximately 10%. Therefore, a call to action to reduce "defensive SARs" while enhancing their accuracy and informational content is crucial for the system to progress.

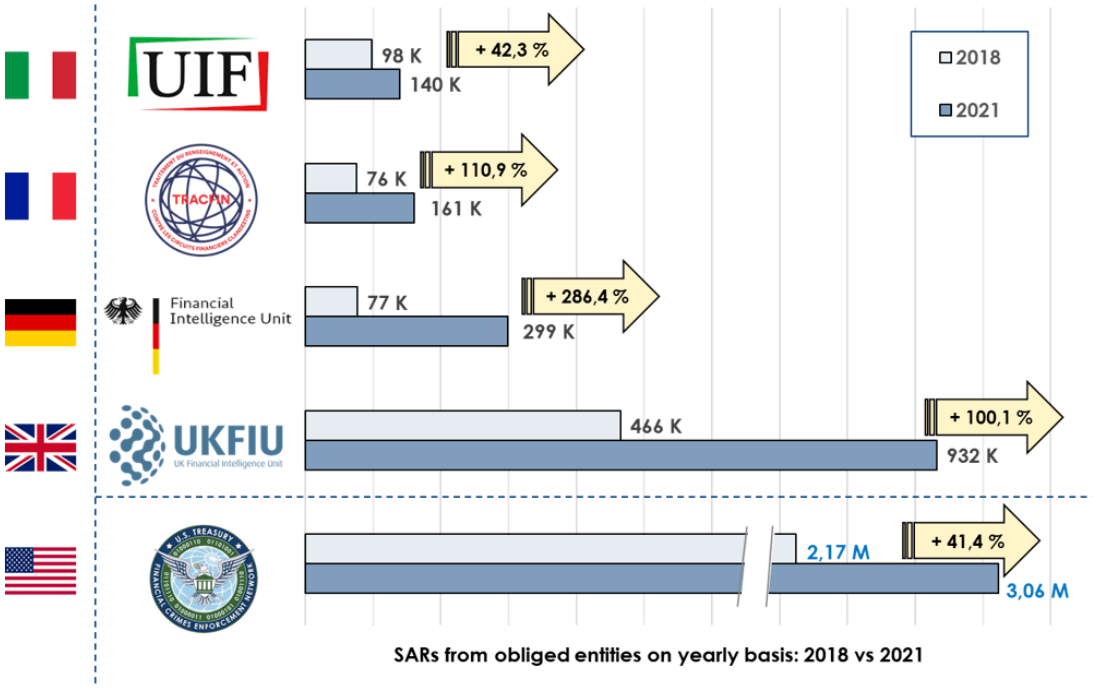

Figure 4.11: Relentless growth of SARs filing per year

Chapter 5

Innovative approach: Multi-criteria Anomaly Detection

In the context of the curricular internship that I carried out in the Models, Analytics and Special Investigation office of the Anti financial Crime Department of Intesa Sanpaolo Group, I had the opportunity to develop a new algorithm for monitoring the wire transfer activity, either SEPA or SWIFT. This has been made in order to improve the monitoring power of the current systems that, as the vast majority of the industry, is affected in a certain degree by some of the gaps already mentioned in Chapter 4.

In this case, Intesa Sanpaolo has undertaken an internal Research & Development initiative leveraging skills and tools of its AFC MAS office. Indeed, the Bank makes extensive usage of both vendor-supplied systems as well as internally develop ones since with the creation of MAS office in 2017, it has acquired the capacity to independently perform the entire end-to-end process for transaction monitoring development ranging from risk intelligence to algorithm design, testing and "go-pro" support. While vendor-supplied systems are supposed to be easier to roll-out and expected to cover all the most recurrent AML/CFT risk categories, when it comes to complex matters in which the degree of customization and integration with legacy system is crucial, the internal R&D option is a preferred way to achieve tailor-made solutions with unparallel speed and effectiveness.
The context of wire-transfers, correspondent banking entangled with cross-border issues, is such a case to be dealt with the latter that basically exploit one of the largest data-warehouse in the banking sector in Italy (the Intesa Sanpaolo "BFD" that stands for Big Financial Data) combined with a leading general purpose

statistics, data mining and data analysis software (SAS) that enable the MAS team to implement detection logics as well as to leverage proprietary dataset to pinpoint "anomalous" traffic among the "expected" one. In the peculiar case of the current dissertation, it has to be mentioned that several innovative breakthrough are at stake, starting from the general algorithm architecture that steams from an innovation challenge deployed jointly by Intesa Sanpaolo and the Department of Control And Computer Engineering (DAUIN) of Politecnico di Torino under the umbrella agreement of the Anti Financial Crime Digital Hub consortium. The name of the algorithm, MAD1, comes from this project (Multi-criteria Anomaly Detection) that, at the time being, is in the second phase of its running.

The following chapters will deeply analyze the perimeter and the logics beyond the algorithm highlighting the innovation which it incorporates and which makes it the pioneer of a new concept of design.

5.1 Engagement description

Chapter 4 widely went through the pain points of the actual transaction monitoring system belonging to different perspective. This chapter's aim is to briefly recap which they are, which level they affect and which aspect they concern in order to introduce the solution proposed by the Models, Analytics and Special Investigation office of Intesa Sanpaolo.
Assuming a macro view, the two main effects coming out from the system are the working overload of the UIF and the very high rate of false positive SARs coming out from the obliged entities, especially financial institutions. This two effects can be summarized in a necessity, and explicit request, of the UIF to have a lower number of SARs transmitted embodying more valuable investigational payload.
A first provision issued by UIF to face this problem has been the imposition to all the obliged entities such that a SAR can be sent only if it reflects either a subjective and objective indicator. 1.5.1

The causes of these two macro-effects can be traced back to lower granularity dynamics, such as the technical aspect that mono-feature algorithms are weak because, by taking one feature at a time as input, they address the problem without considering the combined effect of multiple factors or the respective weight of one factor relative to all of them.

Other shortcomings that originate in the algorithm's operating mechanism include opacity regarding the intermediate nodes in a correspondent banking payment chain and limited visibility in the context of funneling with a non-customer node.

In fact, current monitoring systems, aimed at monitoring the activity of their own customers, aggregate and analyze the transactions for each of their customers, thus missing any of their own customers involved in transactions that pivot outside their financial institutions.

All of this should be addressed within the fact that wire transfer operations are the prevalent method for money laundering or terrorism financing activities.
This prevalence leads to the necessity of having a dedicated monitoring method, to the extent that a solution has been formulated in collaboration with the Models, Analytics, and Special Investigations office of Intesa Sanpaolo.

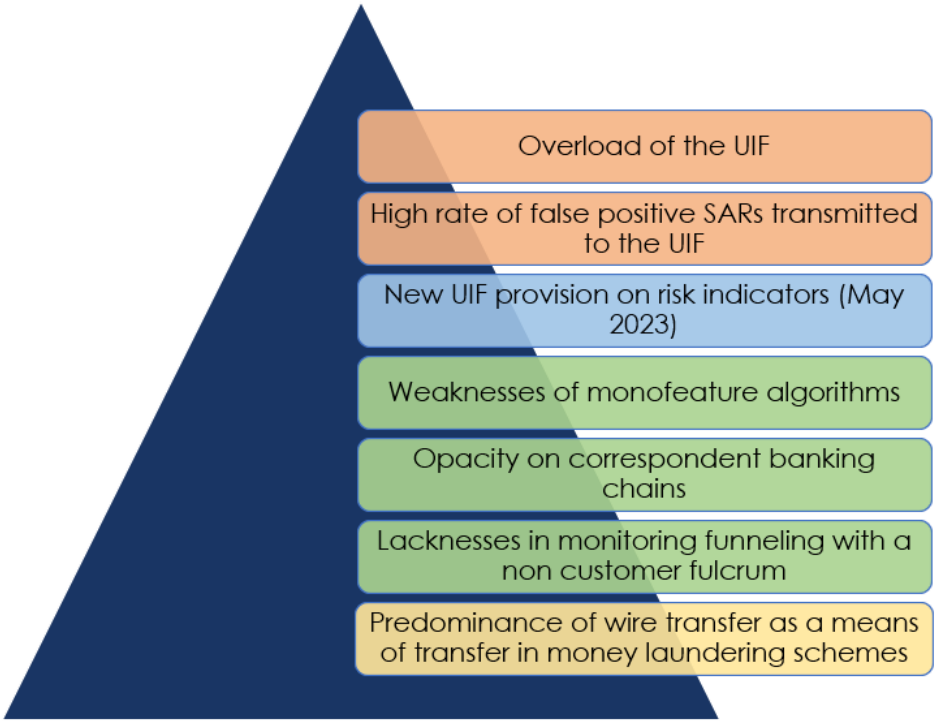

Figure 5.1: Macro and micro pain points of the actual monitoring system

5.2 Design and workflow of the algorithm

The Multi-criteria Anomaly Detection (MAD1) algorithm, as the name suggests, introduces a multi-feature approach, where multiple features serve as inputs for the monitoring algorithm. This section delves into a detailed examination of the algorithm's construction, dissecting each step of the pipeline (Figure 5.2).

The preliminary step to the operational pipeline of the algorithm involves creating a comprehensive list of features that capture suspicious activities associated with cross-border or local wire transfers. This compilation is guided by the recommendations provided by the UIF and categorized within the Red Flag Themes (Figure 4.1).
A substantial number of features designed for the algorithm are listed in Table 5.1; however, some features cannot be disclosed due to business confidentiality.

Each feature's name is designed to be self-explanatory, yet it is crucial to delve into the details of each feature to establish a comprehensive framework.

Regarding the *High Risk Geography* Red Flag Theme, it is manifested through eight distinct features (F01 to F08). F01, "Unexpected intermediary in High Risk Geography", checks if, in a transaction, one of the two counterparties belongs to a High-Risk Geography. Features F02 to F07 focus on the counterparty, examining its residence country or bank country to determine if they belong to a country classified as a High-Risk Geography, Tax Haven, or Terrorist Haven. F08 identifies inconsistencies between the counterparty's country and the counterparty's country bank.
F09, "Round amount per thousand", serves as an indicator of a *Lack of Economic purpose* indicator, identifying transactions with this characteristic. F15, "Smurfing 1-1", within the same theme, detects behavior where individuals attempt to circumvent thresholds by dividing a certain sum into multiple transactions.
F10, "Amount compatible with structuring", aims to identify cases where individuals try to stay just below thresholds that require compulsory registration and belongs to *Structuring* red flag theme. The "Velocity" feature, F11, homonymous to its category of belonging, detects instances where funds are received shortly after giving away a similar amount.
F12 and F13, related to *Funneling*, attempt to identify cases in which a counterparty disperses an amount of money by distributing it to multiple counterparts. Chapter 4.4 extensively explains the mechanisms of this behavior.
Lastly, F14 is a feature related to *Identity Concealment*, checking if an individual exhibits different behavior from that of previous months.

N°	Description	Red Flag Theme
F01	Unexpected intermediary in High Risk Geography	High Risk geography
F02	Country of origin of the counterparty in High Risk Geography	High Risk geography
F03	Country of origin of the counterparty in Tax Heaven	High Risk geography
F04	Country of origin of the counterparty in Terrorist Heaven	High Risk geography
F05	Bank of the counterparty in High Risk Geography	High Risk geography
F06	Bank of the counterparty in Tax Heaven	High Risk geography
F07	Bank of the counterparty in Terrorist Heaven	High Risk geography
F08	Geographical inconsistency between counterparty country and counterparty country bank	High Risk geography
F09	Rround amount per thousand	Lack of economic purpose
F10	Amount compatible with structuring	Structuring
F11	Velocity	Velocity
F12	Funneling $1 \rightarrow N$	Funneling
F13	Funneling $N \rightarrow 1$	Funneling
F14	Transaction beyond a percentage variance	Identity concealment
F15	Smurfing 1-1	Lack of economic purpose

Table 5.1: Features of MAD1 (selection due to information security concerns)

Once the list of features is formulated, MAD1 enters the pipeline (Figure 5.2), which has been divided into four main phases:

1. Restyle of a table of transactions containing the interested fields.
2. Aggregation on the not customer counterparty and restyle of a table of counterparties.
3. Calibration of tunable parameters.
4. Filtering counterparties in order to obtain detections.

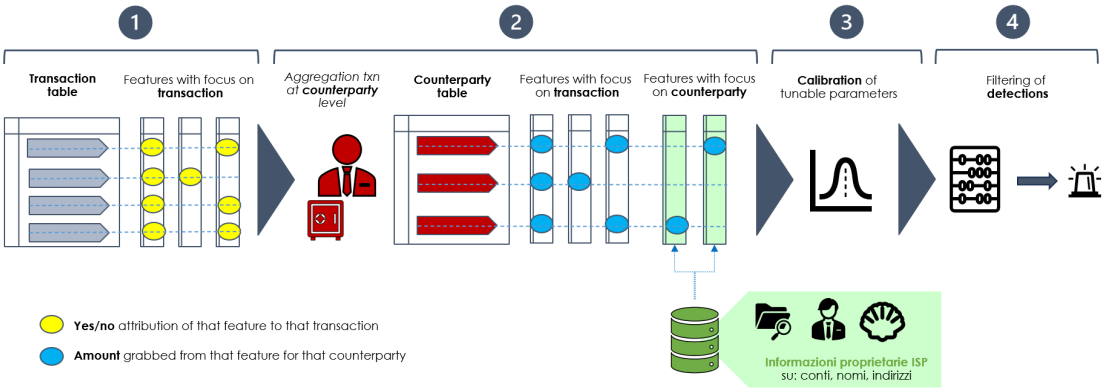

Figure 5.2: Pipeline of the algorithm

Before delving into the detailed description of each step, it is essential to provide a clarifying point that will be beneficial for further understanding.
The MAD1 algorithm takes transactions and features as input. Transactions represent individual fund movements characterized by an originator, a beneficiary, and a specific amount. On the other hand, features denote potential risks derived from the wire transfers activity and are derived from the description of red flag themes. The complexity arises from the fact that risks may emerge from a transaction's characteristic or from one of the counterparties. This distinction, concerning which focus to adopt when matching features and transactions, is a pivotal aspect of the activity.
To illustrate this distinction, consider the features "Round amount per thousand" and "Country of origin of the counterparty in High Risk Geography". Both serve as risk indicators, but they differ in scope. The first relates to a single transaction, while the second affects one of the counterparties involved in the transaction. It's worth noting that stating a feature has a focus on one counterparty is equivalent to asserting that it has a focus on a set of transactions (those with that counterparty as either the beneficiary or the originator).
In Figure 5.3, the distribution of the 15 features based on this logic is illustrated.

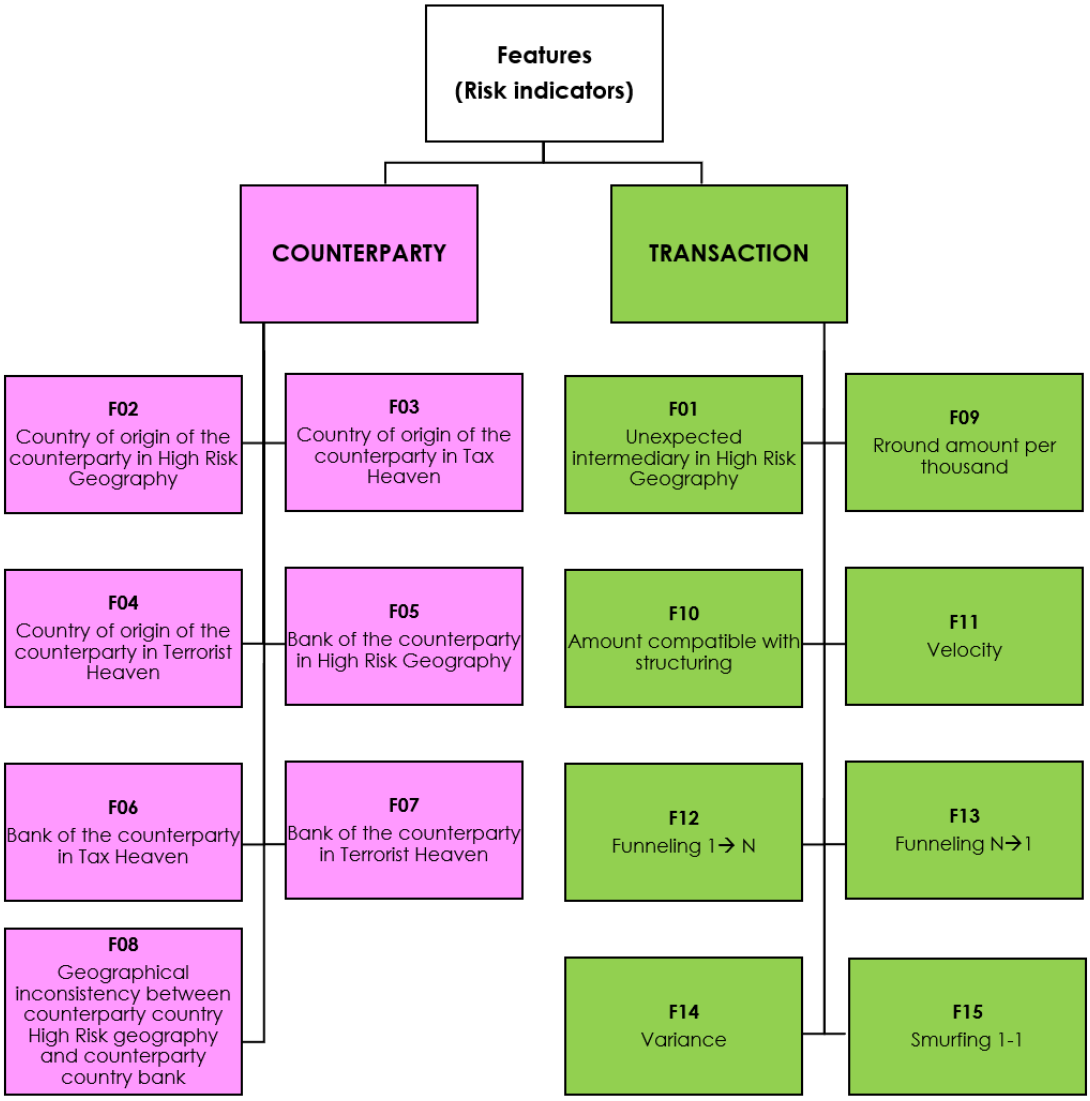

Figure 5.3: Features with focus on transaction vs features with focus on counterparty (selection due to information security concerns)

Now that this fundamental concept has been clarified, it is possible to proceed examining how this algorithm is constructed.

Restyle of a table of transactions

As a first step, a table known as the "transaction table" is created, where each row corresponds to a transaction, and relevant information about the transactions is organized into columns (Figure 5.4). This information includes details such as

the originator, beneficiary, their respective residences, and the countries of their banks, among others.
Additionally, columns related to features with a focus on the transaction are added (in purple). In Figure 5.4, a simplified example illustrates how the table looks once columns with features are added. In this example, features F01, "Unexpected intermediary in High Risk Geography", and F09, "Round amount per thousand", are included. The list of High Risk Geography countries is an internal list drafted by Intesa Sanpaolo, where Gibraltar and Nigeria are considered high risk.
Fields related to features are populated with a yes/no variable at this stage, indicating whether a transaction exhibits the risk indicated by that feature.

For example, in transaction 1, the originator is John, a customer of Bank A located in Gibraltar, and the beneficiary is Sophie, a customer of ISP, an Italian bank. This transaction involves the transfer of 1.000€ from John to Sophie. Feature F01 is triggered because one of the two banks involved in the transaction belongs to a High Risk Geography (Gibraltar), and feature F09 is also triggered as the amount is rounded to thousand.
On the other hand, transaction 3 involves the transfer of 45€ from Bob, an ISP customer, to John, a customer of Bank A in Gibraltar. This transaction triggers F01 due to the presence of Gibraltar but not F09, as the amount is not rounded to thousand.

ID transaction	Originator	Beneficiary	Amount	Originator bank	Beneficiary bank	Originator country bank	Beneficiary country bank	F01 transaction	F09 transaction
1	John	Sophie	€ 1.000,00	Bank A	ISP	Gibraltar	Italy	yes	yes
2	Jack	Laura	€ 158,57	Bank B	ISP	Nigeria	Spain	yes	no
3	Bob	John	€ 45,00	ISP	Bank A	Italy	Gibraltar	yes	no
4	Jenny	Millie	€ 39.000,00	ISP	Bank C	Italy	Italy	no	yes

Figure 5.4: Table of transactions

Restyle of a table of counterparties

A subsequent step involves aggregating transactions based on counterparties that are not customers of Intesa Sanpaolo, aligning with the algorithm's goal to address what is not covered by standard monitoring algorithms (Chapter 4.4). This aggregated table will have a different focus compared to the transaction table and will include different columns. For instance, instead of individual transaction amounts, the table will display the total amount moved by each counterparty. Furthermore, instead of a yes/no variable, the table will indicate the partial amount that triggered a specific feature.
As depicted in Figure 5.5 (the continuation of Figure 5.4), Counterparty 1 (John)

has moved a total of 1.045€, with 1.000€ attributed to transactions triggered by F09.
In this table, additional features with a focus on the counterparty are added (in green). Unlike the transaction table, these features concentrate on characteristics related to the aggregation of transactions rather than individual transactions. Fields are filled with the entire amount moved by the respective counterparty and triggered by that feature. For example, Counterparty 1 has moved a total of 1.045€, and the country of the counterparty's bank triggers F05, "Bank of the counterparty in High Risk Geography." The corresponding cell is populated with 1.045€, the total, as the feature reflects a characteristic of the individual rather than a specific portion of their transactions.

ID counterparty	Counterparty name	Counterparty country bank	# transactions	Counterparty residence	Counterparty country bank	Total amount	F01 transaction	F09 transaction	F02 counterparty	F05 counterparty
1	John	Bank A	2	Italy	Gibraltar	€ 1.045,00	1.045	1.000	0	1.045
2	Jack	Bank B	1	France	Nigeria	€ 158,57	158,57	0	0	158,57
3	Millie	Bank C	1	Gibraltar	Italy	€ 39.000,00	0	39.000	39.000	0

Figure 5.5: Table of counterparties

Calibration of tunable parameters

Subsequently, the process involves the calibration of tunable parameters. A tunable parameter is a metric on which a threshold can be defined. This threshold helps determine whether a specific feature should be attributed to a given counterparty based on whether the parameter's value surpasses the established threshold.

In simpler terms, to identify suspicious counterparties, it is necessary to calibrate each feature and assess its relevance. The most straightforward tunable parameter is the transaction amount. For instance, consider the calibration of F02, i.e., "Country of origin of the counterparty in a High-Risk Geography."
The key question is: When is this feature truly significant?
From the data, the only parameter available for evaluating this feature is the associated transaction amount. So the challenge is to find a so called *de minimis amount* threshold. Intuitively, if F02 is triggered with a very low amount, it is reasonable to assume that this does not pose a significant risk.
However, adopting a scientific approach, to determine the value of the parameter above which the feature is deemed significant, the workflow in Figure 5.6 is repeated for each feature.

The distribution (a) is derived from the counterparty table, as illustrated in Figure 5.7, by selecting values different from 0, as our focus is on the population characterized by the feature. This distribution is then plotted on a graph where

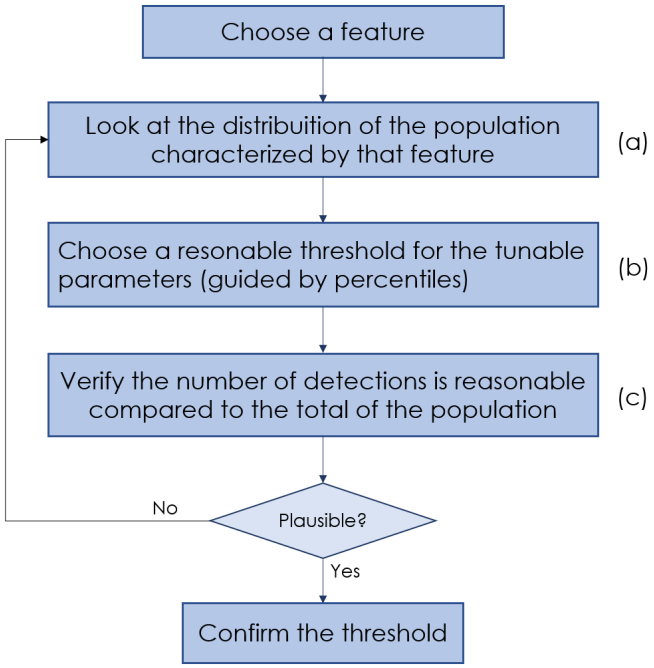

Figure 5.6: Calibration workflow for each feature

the *x-axis* represents the values assumed by the variable "amount", and the *y-axis* indicates the occurrences of each value of amount.

Selecting the appropriate percentile (b) to determine the *de minimis amount* depends on several factors. The goal is to achieve a moderate number of detections with high precision. Choosing a high threshold aligns with the aim of a moderate number but carries the risk of overlooking something important. Conversely, keeping the threshold low provides the security of not missing any relevant cases but increases the number of detections. Considerations such as the meaning of the feature and the size of the population are essential when choosing the percentile. For instance, if the risk of structuring (F10) is significant starting from 15.000€, regardless of the population size, any threshold under 15.000€ is irrelevant. On the other hand, a higher percentile is necessary when dealing with a very large population; otherwise, conducting further analysis becomes impractical.
Another aspect which it's crucial to bear in mind is that we are seeking anomalies and this means that choosing thresholds around the median, or worse, lower, doesn't effectively target behaviors deviating from normality.

Once the threshold is chosen for a feature, it's possible to verify if the number of detections obtained from that feature is plausible compared to the total population (c). This involves dividing the number of detection obtained with that *de minimis*

ID counterparty	...	F01 transaction	F09 transaction	F02 counterparty	F05 counterparty
1	...	1.045	1.000	0	1.045
2	...	158,57	0	0	158,57
3	...	0	39.000	39.000	0
4	...	320	0	51.240	320
5	...	50	0	0	96
6	...	5.842,4	5.000	0	5.842,4
7	...	0	0	5.600	0
8	...	0	48.000	0	48.000

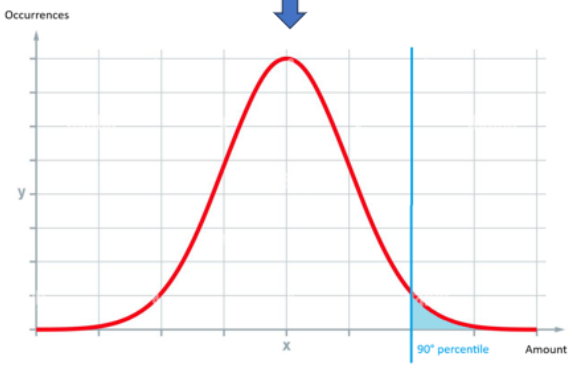

Figure 5.7: Table of counterparties - Features distribution

amount by the total population. Considering that criminal activity is performed by only 0.05% of the entire population, it is advisable to stay under a result of 1%. If the percentage obtained is too high, the process returns to (a), and another threshold is chosen.

To support the discussion, and with the assumption that the numbers provided in the example are entirely arbitrary and certainly not realistic, let's assume that from the study of the distribution of the feature F02, Figure 5.7, a threshold of 40.000 has been deduced for the "amount" parameter. The size of the population related to F02 is 3 (Counterparty 3, 4, 7), and the detections obtained with this threshold for the amount are only 1 (Counterparty 4), as it is the only one that triggered the feature with a significant amount. In this example, the detection rate for F02 would be 0.125 (1/8), considering that the entire population consists of 8

counterparties.

Upon reaching a plausible threshold for each feature, it is possible to proceed to the last step of the pipeline, which is the actual production of detections.

Filtering counterparties in order to obtain detections

To align with the directives outlined in the provision issued by the UIF (1.5.1) on May 12, 2023, which mandates that a Suspicious Activity Report (SAR) must be supported by both objective and subjective indicators, it is possible to categorize features in Table 5.1 into two groups: objective and subjective features. Figure 5.8 clearly shows that classification.

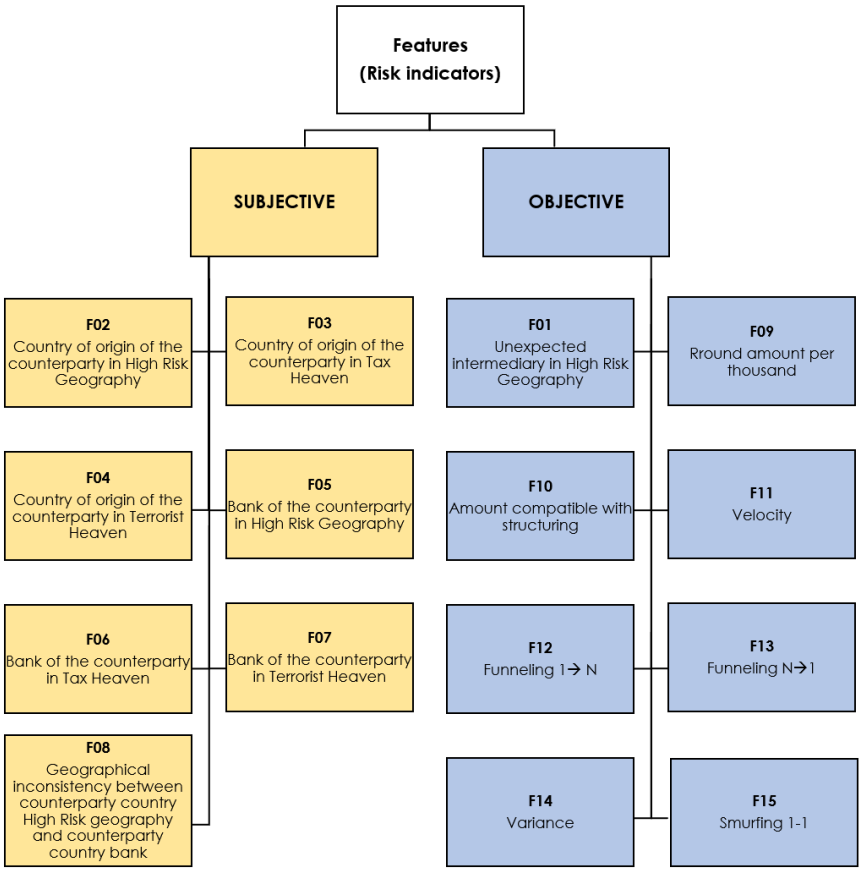

Figure 5.8: Classification of the features in subjective and objective risks indicator (selection due to information security concerns)

From that, it is logic to imagine a last step, which takes in input the counterparties with their relative features already calibrated.
The filter will select (Figure 5.9) just counterparties with:

Consequently, it is logical to envision a final step that takes the counterparties with their respective calibrated features as input. The filter will specifically choose (Figure 5.9) counterparties that meet the following criteria:

1. Have at least one subjective indicator.

2. Have at least one objective indicator.

ID counterparty	...	F01 objective	F09 objective	F02 subjective	F05 subjective	Detection
1	...	x	x	x	x	✓
2	...	x				✗
3	...		x	x		✓
4	...			x	x	✗
5	...	x	x			✗
6	...					✗
7	...	x		x	x	✓
8	...		x			✗

Figure 5.9: Filter on subjective and objective features

From the table provided as an example (5.9), three counterparties meet the specified criteria: counterparty 1, 3, and 7. Counterparty 2 is excluded as it satisfies the requirements of objective indicators but not subjective ones. Counterparty 4, on the other hand, has two features, but none of them falls under the objective class, so it is also excluded. The same reasoning applies to the other excluded counterparties.

5.3 Innovation and performance

This approach introduces three primary innovations. The first involves the simultaneous consideration of a multitude of red flag themes, from which multiple features can be derived. This has a massive impact on the precision of the algorithm, as suspicious activity is flagged only if there is a convergence of evidences that raises suspicion. Moreover, this characteristic aligns the algorithm with the requirements set by the UIF in its most recent publication at the time being (12 my 2023).

The second innovation is the expanded focus on monitoring the activity of counterparties that are not customers of the financial institution conducting the monitoring. This allows for the incorporation of more information and extends the coverage of wire transfer activity.
A third innovation is the increased visibility into correspondent banking chains 3. Unlike the current generation of transaction monitoring systems where visibility was limited to the endpoints of the chain, the algorithm shifts the analysis to each of the counterparties present in the chain.

The algorithm is scheduled to go live in December, so it is not possible to predict the exact performance at this moment. However, given the solid statistical foundations of this algorithm and its targeted and precise approach to uncovering anomalies among millions of transactions, we anticipate a significant improvement in the true positive rate.
Currently, the true positive rate across the banking industry is around 3%, as indicated in 4.6. It is plausible to expect, and it would be groundbreaking in the Anti-Financial Crime sector, to achieve a true positive rate of around 20% with this algorithm. Such a number marks a shift in the monitoring of transactions, making the system significantly more efficient.

Chapter 6

Conclusions and future perspectives

6.1 Future perspectives

Despite MAD1 algorithm bringing significant innovation to the Anti-Financial Crime sector, it represents just one of the initial steps in the process of streamlining the system. This paragraph provides a glimpse into what the near future holds in terms of new topics to explore and implement (Figure 6.1).

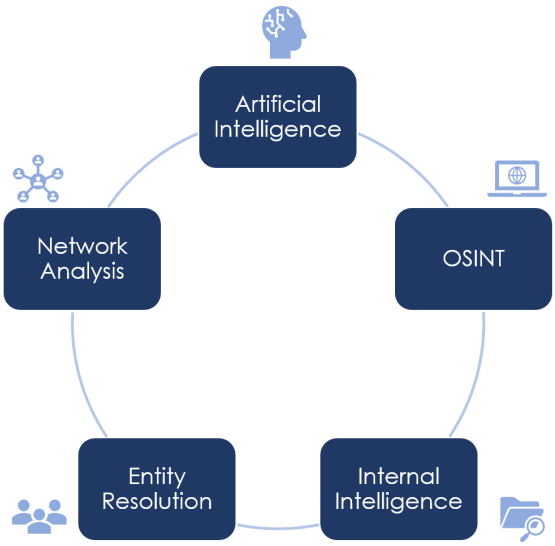

Figure 6.1: Future perspectives in the AML domain

Certainly, the first activity that deserves implementation, as it does not require

proper scientific research but rather integration into existing monitoring systems, is the use of internal intelligence. This encompasses all information that a financial institution possesses, utilizes, and archives through various activities, representing a valuable asset of information. This aspect is achievable also thanks to the transition of payment systems messaging discussed in Chapter 2.2.1. Consequently, clearer and more precise information regarding the parties involved in the transaction will be available.

In the realm of maximizing the use of existing knowledge, Open Source Intelligence (OSINT) is another activity that enriches the information repository at no cost except the injection implementation. OSINT involves gathering information readily available on the web. However, transforming this information into usable data for algorithms would pose a non-trivial challenge.

Another avenue for enhancing the quality of information collected by monitoring systems has been explored in collaboration with the Politecnico di Torino through a project called "Entity Resolution". Leveraging artificial intelligence techniques, this project accurately performs the activity of counterparty resolution.
The Entity Resolution activity, as implied by its name, is the method by which, in proprietary company databases, a name is associated with a non-customer bank account. For customers, this activity is unnecessary as the required information is already available. As discussed in detail in Chapter 2, information arrives through messages, whether SWIFT or other types, allocated to numbered fields. When a user initiates a wire transfer, a message is automatically generated from the user's bank to the destination bank. Some fields of this message, related to the user, are automatically filled by the system. However, fields related to the recipient are partially filled with information entered by the user, leading to non-uniqueness and imprecision.
The name of the counterparty to whom a wire transfer is sent, for example, is one of the fields subject to this imprecision. The same "John Green" could be entered as "John Green," "J. Green," or "Green John."
The Entity Resolution project aims to recognize this ambiguity and link the counterparty's account number to the actual owner's name using rule-based, ontology-based methods, as well as machine-learning techniques like standard classifiers and sequence models. This activity brings significant benefits in terms of increased precision of collected information, enabling better intelligence.

More precise information would also benefit the so-called "Network Analysis" activity, the study of complex systems to identify patterns and trends in entity relationships. This type of activity would broaden the visibility spectrum, making AML activities more accurate and effective.

While ancillary to Entity Resolution and Network Analysis activities but central in dedicated monitoring algorithms, the last area to explore and integrate into anti-money laundering systems is connected to the vast field of Artificial Intelligence (AI). Incorporating AI into AML processes enhances accuracy, reduces false positives, and provides a more proactive and dynamic defense against financial crimes. As the financial landscape continues to evolve, AI stands as a crucial ally in fortifying the resilience of AML frameworks.

6.2 Conclusions

At the time being, we face a landscape marked by the inefficiency of standard transaction monitoring systems among financial institutions obligated to report Suspicious Activity Reports (SAR) to the FIUs. This thesis aim is to propose an innovative approach for transaction monitoring, specifically focusing on wire transfers activity involving Correspondent Banking transactions.
The algorithm has been internally developed in the Intesa Sanpaolo group by the Model, Analytics and Special Investigation Office.
Despite the focus on the wire transfer activity, the algorithm, referred to as Multi Criteria Anomaly Detection (MAD1), is considered scalable, allowing for potential extension to other types of transactions.
MAD1 departs from the traditional "one monitoring algorithm for one risk indicator" approach, adopting a "one monitoring algorithm for multiple risk indicators" strategy. The goal is to reduce the false positive rate by labeling transactions as anomalies when triggering multiple risk indicators simultaneously.
Simulations conducted with historical data indicate a significant reduction in the number of detected anomalies compared to previous systems. This reduction is a positive sign, as the point of weaknesses of the actual system are the wide number of detections and few true positives. Encouraging estimates also exist for the decrease in false positives, potentially reducing the UIF-reported 3% to 20%. Lastly, as MAD1 is a proprietary algorithm, it exhibits flexibility, making it easily modifiable and integrable with new data and technologies. In this regard, the algorithm proves to be AI-friendly, accommodating future developments and enhancements.

Bibliography

[1] «Europol. Available online: https://www.europol.europa.eu/». In: () (cit. on p. 3).

[2] A. Bongani Sibindi W. Gaviyau. «Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: A Critique». In: *Journal of Risk and Financial Management* (2023) (cit. on pp. 3, 4).

[3] M Starnini, Ch Tsourakakis, D Moncalvo, et al. «Smurf-Based Anti-money Laundering in Time-Evolving Transaction Networks». In: *Joint European Conference on Machine Learning and Knowledge Discovery in Databases* (2021) (cit. on p. 4).

[4] R Soltani, U.T Nguyen, Y Yang, M Faghani, A Yagoub, and A An. «A new algorithm for money laundering detection based on structural similarity». In: *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (2016) (cit. on p. 4).

[5] B Unger, M Siegel, J Ferwerda, W de Kruijf, M Busuioic, K Wokke, and G Rawlings. «The amounts and the effects of money laundering». In: *Report for the Ministry of Finance* (2006) (cit. on p. 4).

[6] C. Clemente G. Castaldi. «La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli». In: Quaderni dell'antiriciclaggio, Analisi e studi 20 (Mar. 2023). Ed. by UIF (cit. on pp. 4, 9, 11, 16).

[7] «FATF. Available online: https://www.fatf-gafi.org/». In: () (cit. on pp. 6, 9, 31).

[8] A. Zerden. «Demystifying the Financial Action Task Force». In: (Sept. 2022). Ed. by Lawfare (cit. on p. 6).

[9] «International standards on combacting money laundering and the financing of terrorism & proliferation». In: FATF Recommendations (Feb. 2023) (cit. on pp. 6, 51).

[10] «EUR-Lex. Available online: https://eur-lex.europa.eu/homepage.html». In: () (cit. on p. 9).

[11] «Documentazione in materia AML Package». In: (2023). Unpublished document (cit. on p. 11).

[12] G. Pavilidis. «The birth of the new anti-money laundering authority: harnessing the power of EU-wide supervision». In: *Journal of Financial Crime* (Sept. 2023) (cit. on pp. 12, 13).

[13] «Regole in materia di monitoraggio transazionale e di segnalazioni di operazioni sospette per il contrasto del riciclaggio e del finanziamento del terrorismo». In: (2021). Unpublished document (cit. on p. 20).

[14] «Investopedia. Available online: `https://www.investopedia.com/`». In: () (cit. on pp. 23, 32).

[15] «Bankit. Available online: `https://www.bancaditalia.it/`». In: () (cit. on p. 25).

[16] «EBA CLEARING. Available online: `https://www.ebaclearing.eu/`». In: () (cit. on p. 25).

[17] «MEF. Available online: `https://www.bis.org/`». In: () (cit. on p. 31).

[18] «Closing the loop: AML/CFT supervision of correspondent banking». In: (2020). Ed. by BIS (cit. on p. 34).

[19] «Correspondent Banking services». In: FATF Guidance (2016) (cit. on pp. 34, 39, 40).

[20] FATF. «Survey Results on Implementation of the FATF Standards». In: (2021) (cit. on p. 39).

[21] «Correspondent Banking». In: (2016). Ed. by BIS (cit. on p. 39).

[22] «Wolfsberg Group. Available online: `https://wolfsberg-group.org/`». In: () (cit. on p. 42).

[23] the Wolfsberg Group. «Wolfsberg Financial Crime Principles for Correspondent Banking». In: FATF Guidance (2016) (cit. on p. 42).

[24] MAS. «Automated Transaction Monitoring scenarios management - Handbook». In: (). Unpublished document (cit. on pp. 44, 46).

[25] «Quaderni dell'antiriciclaggio - Collana Dati statistici I-2023». In: (). Ed. by UIF (cit. on p. 48).

[26] Jim Richard. «Rules-Based Monitoring, Alert to SAR Ratios, and False Positive Rates – Are We Having The Right Conversations?» In: (2021) (cit. on p. 58).

[27] «Global Anti-Money Laundering Survey 2014». In: (2015). Ed. by KPMG (cit. on p. 58).

[28] «Anti-money laundering (AML) Transaction Monitoring 2018 EMEIA Survey Report». In: (Oct. 2018). Ed. by EY (cit. on p. 58).

[29] «AML Transaction Monitoring — 2020 Nordic Survey Report». In: (Feb. 2021). Ed. by EY (cit. on p. 58).

[30] P. Giuliani. «Why Consider Machine Learning For Transaction Monitoring?» In: (Feb. 2023). Ed. by Guidehouse (cit. on p. 58).

[31] «McKinsey Benchmark, internal document prepared for Intesa Sanpaolo». In: (2023). Ed. by McKinsey. Unpublished document (cit. on p. 58).

[32] A. Meyer A. Murphy S. Boezio. «Cleaning up money laundering - banks need less expensive and more reliable ways to detect illicit transactions». In: (2017). Ed. by Oliver Wyman (cit. on p. 58).

[33] «The risk and the benefits of using ai to detect crime». In: (Aug. 2018). Ed. by Oliver Wyman (cit. on p. 58).

[34] «False Negatives: The Danger that Lurks Within». In: (May 2022). Ed. by SymphonyAI (cit. on p. 58).

[35] «FinCEN. Available online: `https://www.fincen.gov/reports/sar-stats`». In: () (cit. on p. 59).

[36] «Annual Report 2021». In: (May 2023). Ed. by FIU - ZOLL (cit. on p. 59).

[37] «AML/CFT: reporting entities activity 2022 review». In: (2022). Ed. by des finances et de la souveraineté industrielle et numérique Ministère del l'éeconomie (cit. on p. 59).

[38] «Rapporto Annuale 2022». In: (May 2023). Ed. by UIF (cit. on p. 59).