2024



National Risk Analysis

ADENDA 2024. PUBLIC VERSION

CONTENTS

1. INTRODUCTION. 3
2. METHODOLOGY. 3
2.1. Participating institutions. 4
2.2. Identification of risks, threats and vulnerabilities. 5
3. REGULATORY AND INSTITUTIONAL FRAMEWORK. 7
3.1. Regulatory framework: FATF, the European Union and national regulations. 7
3.3. Preventive framework: national coordination. 8
3.4. National framework for Money Laundering/CFT supervision. 9
3.5. Investigation and prosecution framework. 10
4. ANALYSIS OF KEY DEVELOPMENTS: THE IMPACT OF THE COVID-19 PANDEMIC AND THE WAR BETWEEN RUSSIA AND UKRAINE. 12
4.1. The impact of the COVID-19 pandemic. 12
4.2. The impact of the war between Russia and Ukraine. 13
5. MAJOR THREATS RELATED TO MONEY LAUNDERING. 14
5.1. Organised crime. 14
5.2. Drug trafficking. 19
5.3. Economic and financial crimes: fraud, tax offences, and cases linked to corruption. 21
5.4. Money Laundering by third parties and from offences committed abroad. 23
6. MAIN THREATS RELATED TO TERRORIST FINANCING. 24
6.1. Jihadist terrorism. 26
6.2. Terrorist Financing for jihadist terrorism. 27
6.3. ETA terrorism. 28
6.4. Other terrorist groups. 29
6.5. National Counter-Terrorism Strategy. 29
7. MAIN VULNERABILITIES IN Money Laundering AND Terrorist Financing. 30
7.1. Vulnerabilities arising from the population. 30
7.2. Vulnerabilities arising from geographical factors. 31
7.2.1 Conducting transactions with high-risk territories or with citizens/entities from those territories. 31
7.2.2. Transactions with countries at higher risk of Terrorist Financing. 32
7.2.3. Activities in the Gibraltar area. 32
7.3. Vulnerabilities arising from the nature of the organisation or the activity carried out. 33
7.4. Vulnerabilities arising from payment methods, the use of cash and the informal economy. 34
7.5. Vulnerabilities arising from technological innovations in financial transactions. 35
7.5.1. Vulnerabilities arising from the use of cyberspace. 35
7.4.2 Vulnerabilities arising from the use of virtual currencies and assets. 36
8. SECTOR-SPECIFIC RISKS. 36
8.1. Financial sector risks. 37

a) Investment services, collective investment undertakings and management companies. 37
b) Money transfers by payment institutions. 42
c) Other services provided by payment institutions. 46
d) Electronic money transactions. 49
e) Crypto-assets and crypto-asset service providers. 51
f) Use of cash, cash movements and cash-intensive businesses. 56
8.2. Risk in non-financial sectors. 62
a) Activities carried out by notaries. 62
b) Activities carried out by land, commercial and movable property registrars. 65
9. RISKS OF NON-IMPLEMENTATION OR CIRCUMVENTION OF INTERNATIONAL FINANCIAL SANCTIONS. 71
9.1. Concept of international financial sanctions. 71
9.2. International financial sanctions relating to terrorism and Terrorist Financing. 72
9.3. International financial sanctions relating to the proliferation of Weapons of Mass Destruction (WMD). 72
9.4. Vulnerabilities and sector-specific risks. 74
9.5. Conclusions. 76
10. MEASURES TAKEN. 77
10.1. General measures adopted. 77
10.2. Other specific mitigation measures. 78
11. CONCLUSIONS. 83
12. STATISTICS. 85
Abbreviations used 86
List of key regulatory provisions 88

1. INTRODUCTION.

Article 7 of Directive (EU) 2015/849[1] of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of Money Laundering or Terrorist Financing (hereinafter, the Fourth Directive) establishes the obligation to draw up and publish a national risk analysis. Similarly, the Financial Action Task Force (hereinafter 'FATF') sets out in its Recommendation 1 that countries have a duty to identify, assess and understand the risks of Money Laundering and Terrorist Financing (hereinafter 'ML' and 'TF' respectively).

These premises were set out in the National Risk Analysis (hereinafter NRA) published in full in 2020. This new publication will provide an update on existing threats and vulnerabilities at national level, as well as on the sectors facing risks that have emerged since the previous report.

The update to this document, based on new variables affecting certain sectors, is designed as a national strategy to identify new threats, vulnerabilities and potential risks affecting those sectors, with the aim of highlighting the mitigating measures that have been put in place or that may be put in place to address these risks.

The aim of this analysis is therefore to carry out a partial update of the 2020 NRA, given that certain sectors have not experienced substantial changes in the risks identified in the previous study, have not been affected by significant regulatory updates, nor have they been threatened by recent or new criminal activities that could compromise their preventive systems. Since 2020, events such as the COVID-19 pandemic, the Russia-Ukraine war, and the entry into the financial system of new players—such as crypto-asset service providers (hereinafter 'CASPs'), *fintech* companies acting as intermediaries in financial services, and new payment service providers— —are events that have presented new challenges faced by both institutions and authorities at national and international level in the field of Money Laundering/CFT.

These developments have led to the evolution of Money Laundering/Terrorism Financing (ML/TF) techniques and methods, which rely on exploiting vulnerabilities in national systems. This requires, as already noted in the 2020 NRA, a continuous updating of analyses and controls to enable authorities and regulated entities to identify changes in modus operandi, new typologies, ways in which technological advances are being utilised, and developments in the types of jurisdictions that pose a risk in these areas.

As a result of this updated analysis, the authorities will have up-to-date tools to adopt new mitigation measures, adapt the regulatory framework to the identified needs, strengthen the resources deployed, and improve internal coordination and international cooperation, in both preventive and law enforcement contexts. Finally, an assessment will be carried out of the measures adopted in the 2020 NRA and of those that have been implemented, with the aim of analysing compliance with these proposals.

2. METHODOLOGY.

In preparing this document, in accordance with the FATF Guidance on the identification and assessment of Money Laundering/Countering Financing of Terrorism (AML/CFT) risks and the Fourth Directive, various national and international sources of information have been taken into account, and consultations have been held with the

[1] Member States must: make a summary of their national risk assessments available to the public; make the results of their risk assessments available to the European Commission, supervisory authorities and other Member States; prepare their national risk analysis taking into account the European Commission's Report on the Supranational Risk Assessment of Money Laundering and Terrorist Financing affecting the market and relating to cross-border activity, published on 26 June 2017, the second version of which was published in July 2019. https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF.

competent public authorities in each area and with representatives of the private sector. Specifically, this document is based on:

a) The National Risk Analysis for Spain published in 2020.
b) The 2023 Sectoral Risk Analysis of Crypto-assets and Crypto-asset Service Providers.
c) The 2022 National Security Strategy, coordinated by the Department of National Security and issued by the Prime Minister's Office.
d) The National Strategy against Organised Crime and Serious Crime and the National Strategy against Terrorism, coordinated by the Centre for Intelligence against Terrorism and Organised Crime (CITCO).
e) The various existing sectoral risk assessments, which were evaluated by the FATF in 2014, and the follow-up reports from 2017 and 2019.
f) The Supranational Risk Analysis drawn up by the European Union (hereinafter the EU SNRA).
g) The annual reports of public institutions involved in the fight against Money Laundering/TF.
h) The Annual Reports of the National Security Council, submitted annually to the Joint Congress-Senate Committee.
i) Statistics published in these areas, including those relating to prevention, supervision, police investigations and judicial proceedings.
j) Consultations carried out with the various competent authorities in each area of action and documents drawn up by them, some of which are classified.
k) Contributions from representatives of regulated entities and the private sector.

2.1. Participating institutions .

The public institutions involved in drawing up the NRA are:

- State Tax Administration Agency (AEAT).
- Banco de España.
- National Intelligence Centre.
- Centre for Intelligence against Terrorism and Organised Crime (CITCO).
- General Commissariat of the Judicial Police of the National Police.
- General Directorate of Information of the National Police.
- National Securities Market Commission (CNMV).
- General Council of the Judiciary.
- Government Delegation for the National Plan on Drugs.
- Department of National Security.
- Directorate-General for the Regulation of Gambling.
- Directorate-General for Foreign Policy and Security.
- Directorate-General for Legal Security and Public Trust.
- Directorate-General for Insurance and Pension Funds.
- Prosecutor General's Office.
- Special Anti-Drugs Prosecutor's Office.
- Prosecutor's Office of the Audiencia Nacional.
- Special Public Prosecutor's Office for Combating Corruption and Organised Crime.
- Guardia Civil Information Directorate (JI).
- Office for Asset Management and Recovery.
- Secretariat of State for Security.
- General Secretariat of the Treasury and International Finance.

- Executive Service for the Prevention of Money Laundering (SEPBLAC).
- Criminal Intelligence Unit of the Guardia Civil (UTPJ).

2.2. Identification of risks, threats and vulnerabilities .

This analysis follows the methodology established in 2020 for identifying risks, threats and vulnerabilities at national level. As set out in the previous NRA, in order to establish Money Laundering/Terrorism Financing (ML/TF) risks, it is necessary to identify: (i) the threats present in Spain, (ii) the vulnerabilities in the system and the country's context that enable these threats to carry out their activities; and (iii) the sectors (economic and non-economic) and the types of entities and legal structures that may be used or exploited by these threats to perpetrate Money Laundering activities by taking advantage of existing vulnerabilities.

In addition to these variables, this addendum has taken into account endogenous factors influencing the risks arising from the economic and social circumstances that have affected the system in recent years. This includes, for instance, the effects of the COVID-19 pandemic and the war in Ukraine on Money Laundering/Terrorism Financing (ML/TF).

The definitions set out in the previous NRA – which are based on the international standards promoted by the FATF – are adopted for the identification of threats, vulnerabilities and risks, as well as the aspects to be taken into account when determining the vulnerabilities and risk factors indicated for the definition of inherent and residual risk.

"Threats" are those individuals, groups of people or their activities that pose a potential danger due to their capacity to cause harm to the State, society, the economy or other fundamental aspects of a country's life.

Given that threats have criminal and destabilising aims, their analysis in the context of Money Laundering/CFT must primarily take a law enforcement approach, through assessment by the authorities responsible for investigating and prosecuting criminal activities, such as the police authorities (the Directorate-General of the Policía Nacional, the Guardia Civil or regional police forces), the Centre for Intelligence against Terrorism and Organised Crime (hereinafter CITCO), the National Intelligence Centre (hereinafter CNI), the Prosecutor General's Office, judges and courts, or the State Tax Administration Agency (hereinafter AEAT) in matters relating to customs and taxation.

"Vulnerabilities" are those situations and circumstances that may be exploited or utilised by organisations or individuals seeking to carry out Money Laundering or Terrorist Financing activities.

In order to identify these inherent vulnerabilities within the system, various factors that could be exploited for the commission of unlawful activities have been analysed. The following aspects have been taken into account in relation to these vulnerabilities:

- Geographical factors.
- Demographic.
- Technological.
- Those arising from the activity carried out, its regulation and its prudential supervision, as well as in relation to the prevention of Money Laundering and terrorist financing.
- Those arising from the type of legal entity: size, business model, national/international presence, exposure to higher-risk customers, etc.
- Those arising from payment methods, the use of cash and the informal economy.

Furthermore, an individualised analysis has been carried out of the impact that these vulnerabilities have on each of the different financial and non-financial sectors, their activities, corporate structures and other elements and operations that could be exploited by various threats for Money Laundering/TF purposes, leading to an assessment of the risk level for each of them.

Consequently, each chapter analyses the risks associated with activities, sectors and types of institutions, taking into account the threats identified, the characteristics, context, business volume, main vulnerabilities and risk exposure of each. To this end, consideration is given to their vulnerabilities arising from endogenous and exogenous risk factors, as well as their inherent risks and residual risks:

a) 'Endogenous' risk factors are those that are intrinsic, arising from the nature and characteristics of the sector, which may allow or facilitate access to or control by criminals; for example, by setting up or acquiring an entity for the purpose of using it for Money Laundering, or by recruiting an employee or agent.
b) 'Exogenous' risk factors are external factors associated with the potential misuse by third parties of the services, channels or products offered by the sector; for example, through a customer's use, for Money Laundering purposes, of legitimately provided commercial or financial services.

<table>
<tr><th colspan="2">Risk factors</th></tr>
<tr><th>Endogenous</th><th>Exogenous</th></tr>
<tr><td>Establishment or control of an entity for the purposes of Money Laundering/TF.</td><td rowspan="2">Associated with the misuse of services/channels/products by customers or parties involved in transactions for Money Laundering or terrorist financing purposes.</td></tr>
<tr><td>Identification of disloyal agents or employees.</td></tr>
</table>

The outcome of this analysis is an assessment of the various types of risk affecting each sector of activity, taking into account the type of natural or legal persons operating in that sector, the products it markets, the services it provides, the characteristics of its customers and the countries in which it operates. In addition to the specific nature of their operations and services, factors such as information gathered from supervisory experience, knowledge of the activity gained through routine and ad hoc communications, and reports from external experts, amongst other sources, are assessed.

Specifically, for each sector, type of institution or activity, the **inherent risk** of it being used for Money Laundering/Terrorism Financing purposes due to its specific vulnerabilities and characteristics is determined. This inherent risk is adjusted in line with the mitigating measures adopted at national level for that sector, taking into account factors such as its prudential regulation, level of supervision, criminal prosecution, the sector's understanding of risks, the extent to which Money Laundering/Fraud prevention measures are implemented, and the quality of its internal control procedures.

It is these mitigation measures that enable the **residual risk** of sectors, entities and activities being used for Money Laundering/Terrorism Financing-related purposes to be determined.

In accordance with the risk level classification established by the European Commission in the **Supranational Risk Analysis on Money Laundering and Terrorist Financing** (EU SNRA), the risk levels in this analysis may be classified as:

- Low.
- Moderate.
- Significant.
- High.

3. REGULATORY AND INSTITUTIONAL FRAMEWORK.

3.1. Regulatory framework: FATF, the European Union and national regulations.

The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 with the aim of combating Money Laundering and terrorist financing (ML/TF) at a global level. It sets international standards and ensures the effective implementation of legal, regulatory and operational measures to prevent illicit practices relating to ML/TF in both member and non-member countries. The FATF Recommendations, which have been updated on several occasions, serve as the benchmark for assessing the effectiveness of national systems in preventing Money Laundering and terrorist financing, as well as providing the basis for updates to European legislation and the main driver behind amendments to national legislation.

The Fourth Anti-Money Laundering Directive ([2]) incorporates the new provisions adopted by the FATF in 2012, establishing a general framework that must not only be transposed but also supplemented by Member States. Directive (EU) 2018/843 of 30 May (hereinafter the Fifth Directive) amends and updates this framework, extending it to new sectors such as virtual currency exchange service providers and electronic wallet custody service providers, introducing measures to increase transparency regarding company ownership and strengthen the system for identifying beneficial owners, with new assets subject to reporting to the FTF, and broadening the concept of a person with public responsibility, amongst other aspects. Spain's commitment to combating Money Laundering and terrorist financing has led to the successive adoption of various regulatory initiatives and the transposition into Spanish law of the Directives mentioned in the preceding paragraphs. In this regard, Law 10/2010 of 28 April, Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), has been amended in 2013[3] , 2018[4] , 2021[5] , 2022[6] and 2023[7] .

Furthermore, Royal Decree 304/2014 of 5 May, which approves the Regulations implementing Law 10/2010 of 28 April, completes the risk-based approach of the Money Laundering/Terrorism Financing prevention regulations in Spain, incorporating the main new provisions of the international standards adopted by the FATF in 2013.

Alongside these two pieces of legislation, which form the legal framework for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) at national level, the main regulatory provisions of a punitive nature are set out in the Criminal Code, which underwent successive amendments in 2015, 2019 and 2022, both in relation to the criminalisation of Money Laundering and that of terrorism and its financing.

In addition to, or directly linked with, the above legislation, there is a wide range of provisions applicable to Money Laundering/CFT matters, covering both preventive and punitive aspects, with varying legal standing, which are listed in the section entitled 'List of key regulatory provisions'.

---

[2] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of Money Laundering or Terrorist Financing.

[3] Law 19/2013 of 9 December on transparency, access to public information and good governance.

[4] Royal Decree-Law 11/2018 of 31 August transposing directives on the protection of pension commitments to employees, the prevention of Money Laundering, and entry and residence requirements for third-country nationals.

[5] Royal Decree-Law 7/2021 of 27 April transposing European Union directives on competition, Money Laundering, credit institutions, telecommunications, tax measures, the prevention and remediation of environmental damage, the posting of workers in the provision of cross-border services, and consumer protection.

[6] Law 18/2022 of 28 September on the creation and growth of enterprises and Organic Law 9/2022 of 28 July establishing rules to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of criminal offences.

[7] Law 2/2023 of 20 February regulating the protection of persons reporting regulatory breaches and combating corruption.
Royal Decree-Law 5/2023 of 28 June, adopting and extending certain measures in response to the economic and social consequences of the war in Ukraine, in support of the reconstruction of the island of La Palma and other situations of vulnerability; transposing European Union Directives on structural changes to commercial companies and the work-life balance for parents and carers; and on the implementation and enforcement of European Union law.

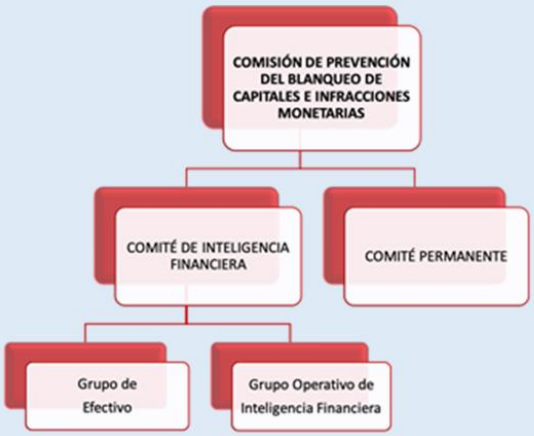
3.3. Preventive framework: national and n coordination.

The Commission for the Prevention of Money Laundering and Monetary Offences (hereinafter COPBLAC) is the body responsible for promoting, developing and coordinating national policies on the prevention of Money Laundering/TF and is involved in imposing sanctions for non-compliance with the Money Laundering/TF prevention obligations set out in Law 10/2010 of 28 April. It comprises 26 members from the main national institutions involved in the fight against Money Laundering and terrorist financing.

CHAIR OF THE COMMISSION Secretary of State for the Economy and Business Support.
MEMBERS Director-General of the Treasury and Financial Policy. Chief Prosecutor of the Audiencia Nacional. Chief Prosecutor of the Anti-Drugs Prosecutor's Office. Chief Prosecutor of the Public Prosecutor's Office for Combating Corruption and Organised Crime. Member of the General Council of the Judiciary. Secretary-General of the Banco de España. Director of Supervision at the Banco de España. Director-General of the Legal Service of the National Securities Market Commission. Director-General of Insurance and Pension Funds. Director-General of Trade and Investment. Director-General of Legal Affairs and Public Trust. Director-General for Foreign Policy and Multilateral, Global and Security Affairs. Director of the Spanish Data Protection Agency. Chief of Staff to the Secretary of State for Security. Commissioner-General of the Judicial Police of the Polic□a Nacional. Chief of the Judicial Police of the Guardia Civil. Director of Intelligence at the CNI. Director of Customs and Excise at the AEAT. Director of the Department of Financial and Tax Inspection at the AEAT. Director of the Basque Autonomous Police (Ertzaintza). Director of the Navarre Regional Police. Director-General of the Policía Nacional of the Government of Catalonia – Mossos d'Esquadra. Director of the Commission's Executive Service – SEPBLAC.
COMMISSION SECRETARIAT Deputy Director-General for Inspection and Control of Capital Movements. Directorate-General for the Treasury and Financial Policy.

COPBLAC meets at least twice a year and operates either in plenary session or through its subordinate committees: the Standing Committee and the Financial Intelligence Committee.

CUADRO 1. Coordinación Nacional



The Standing Committee is primarily responsible for coordinating supervisory activities. It receives and analyses inspection reports drawn up by supervisors, which detail the level of compliance with Money Laundering and counter-terrorist financing (AML/CTF) regulations by regulated entities. It is responsible for initiating disciplinary proceedings for breaches in this area and for issuing improvement notices to regulated entities.

The Financial Intelligence Committee deals with the more operational aspects and the analysis of risks, trends and vulnerabilities. It is supported by a technical body, the GOIF, and by a working group specialising in risks and measures relating to cash movements and means of payment (the Cash Group).

The Commission and its subordinate committees are supported by the Commission Secretariat and the Commission's Executive Service, SEPBLAC.

The Commission's Secretariat falls under the Sub-Directorate-General for the Inspection and Control of Capital Movements within the Directorate-General for the Treasury and Financial Policy, which, amongst other functions, is responsible for conducting disciplinary proceedings for breaches of obligations relating to the prevention of Money Laundering/Terrorism Financing (ML/TF) and for formulating proposals for resolutions, as well as for proposing, drawing up and following up on improvement requirements communicated to regulated entities.

The Commission's Executive Service (SEPBLAC) is the Financial Intelligence Unit in Spain and the national supervisory authority for the prevention of Money Laundering and terrorist financing. It is responsible, amongst other functions, for receiving reports submitted by regulated entities, analysing the information received, assisting the judicial authorities, supervising regulated entities and issuing the reports required by law.

3.4. National Money Laundering/CFT supervisory framework .

At national level, SEPBLAC is responsible for supervising compliance with Money Laundering and counter-terrorist financing obligations by regulated entities. In the case of financial institutions, the prudential supervisors of these institutions – **the Banco de España,** the CNMV **and the Directorate-General for Insurance and Pension Funds** (hereinafter 'DGSFP') – also carry out supervisory and inspection functions in the area of Money Laundering/CFT, taking into account the cooperation agreements in place.

Supervisory action in the area of Money Laundering/CFT prevention follows a risk-based approach. Indeed, SEPBLAC's dual role as a financial intelligence unit and as a supervisory authority creates synergies between these two functions; in this dual capacity, the body serves as a key source of information used in assessing risks at national, sectoral and institutional levels.

The supervisory bodies examine the risks, policies, internal controls and procedures relating to Money Laundering/CFT at the institutions. In the case of financial institutions, account is taken of the guidelines approved by the European Supervisory Authorities on risk-based supervision and the risk factors to be considered by obliged entities when applying due diligence measures.

SEPBLAC, as the general supervisor, carries out risk assessments specific to each sector and to each individual institution, and this information is used as the basis for drawing up the Annual Inspection Plan. Risk assessments are updated periodically or whenever financial intelligence information so warrants, in the event of a change of ownership, an increase in shareholding or any other relevant information.

Prudential supervisors also carry out risk-based supervision of Money Laundering and counter-terrorist financing, whereby supervisory plans and resources are allocated to institutions according to their risk profile and supervisory priority.

Furthermore, it is worth noting the coordination between supervisors through the development of a Joint Inspection Plan.

Alongside this national framework, there is a European institutional framework for the supervision of financial institutions, amended by the so-called CRD-V package[8] , aimed at reducing risks to the European financial system and improving cooperation between competent authorities in the prevention of Money Laundering/Terrorism Financing. In particular, it incorporates measures to promote cooperation and the exchange of information between prudential supervisors, competent authorities responsible for preventing Money Laundering and terrorist financing, and financial intelligence units (FIUs). Furthermore, as part of the supervisory review and evaluation process (known as PRES), anti-money laundering and counter-terrorist financing (AML/CFT) issues must be taken into account by supervisory bodies in their risk analyses of financial institutions; any weaknesses identified in this area within the governance model, business activities or business model of institutions in the sector must be reported to the EBA and the national competent authorities responsible for AML/CFT matters. This supervisory framework is set to change in the coming years, as, under the AMLA Regulation pending publication by the EU, a supervisor with centralised powers at EU level will be established to coordinate national Money Laundering/CFT supervisors.

3.5. Investigation and prosecution framework .

Spain has a comprehensive institutional framework for investigation and prosecution comprising: (i) the LEAs, which have the status of judicial police, and (ii) public prosecutors and judges who have been entrusted with the responsibility of ensuring that Money Laundering offences and their predicate offences are properly investigated.

The two main police forces, the Policía Nacional and the Guardia Civil, are responsible for combating all offences, including Money Laundering, under the direction of the Secretary of State for Security (Ministry of Home Affairs). The Customs Surveillance Service, which reports to the AEAT, is also responsible for investigating and prosecuting tax offences, smuggling and Money Laundering associated with these offences, and forms part of the judicial police. Furthermore, Catalonia, the Basque Country and Navarre have their own police forces, which operate under the direction of the authorities of the respective Autonomous Communities.

[8] Capital Requirements Directive and Regulation.

All units and investigation teams within the Judicial Police are authorised to carry out parallel financial investigations relating to their criminal investigations under the supervision of the Judicial Authority and the Public Prosecutor's Office. They may also refer cases to other authorities for further investigation, where deemed necessary, regardless of where the predicate offence was committed. Investigations by the LEAs are coordinated by CITCO and are supported by coordination mechanisms, such as cooperation and information-sharing agreements and joint working groups or teams, to facilitate investigations into priority matters.

The police units specialising in investigating specific predicate offences and related Money Laundering/Terrorism Financing offences are as follows:

- **Policía Nacional:** the General Directorate of the Judicial Police is responsible for investigating and prosecuting cross-border offences, particularly those relating to drugs, organised crime, economic crime, financial crime, technology-related crime and the regulation of gambling; the Central Unit for Economic and Fiscal Crime (hereinafter UDEF) is responsible for investigating and prosecuting criminal activities, both nationally and internationally, relating to economic and fiscal crime, as well as for providing operational coordination and technical support to the respective regional units; and the General Intelligence Directorate (hereinafter CGI), which is responsible for investigating offences related to terrorism and its financing, as well as for their national and international coordination, and for gathering information on these matters for intelligence purposes.
- **Guardia Civil:** the Guardia Civil Information Directorate (hereinafter JI) combats terrorism and its financing in the various provinces across the country through Command Intelligence Groups (GIC), and nationwide through the Intelligence Service, which has an Economic Investigation Section that carries out complex investigations and advises the GICs in this area. The Judicial Police Directorate, which prosecutes Money Laundering, has the Criminal Intelligence Unit (hereinafter UTPJ), which includes a unit responsible for financial intelligence work within its remit. In the various provinces, there are regional judicial police units. At central level, the Central Operational Unit (hereinafter 'UCO') has a specialised investigation team and handles the most complex Money Laundering investigations. The Guardia Civil, in the exercise of its State Fiscal Protection duties, under the authority of the Department of Customs and Excise, carries out—through the Fiscal Service—missions to monitor the movement of goods, including the movement of cash, both within customs premises and at authorised border crossings, as well as throughout the rest of the national territory.
- **State Tax Administration Agency (AEAT)**: the Customs Surveillance Service (hereinafter 'SVA'), which forms part of the Department of Customs and Excise as a Deputy Directorate, has the remit to prosecute and investigate certain offences and infringements relating to tax fraud, smuggling and Money Laundering, acting in this capacity as a judicial police force. The Department of Customs and Excise is the customs authority in Spain and is solely responsible for controls relating to foreign trade, including those concerning the movement of means of payment; to this end, it relies on officials from the Customs Surveillance Service and on the support of the Guardia Civil in the exercise of its functions as the State's tax guardian and in the prevention and suppression of smuggling. The Asset Investigation Unit of the Sub-Directorate-General for Operations, which reports to the Deputy Directorate for Customs Surveillance, is responsible, amongst other tasks, for coordinating the activities of the Customs Surveillance Service in relation to Money Laundering, including cash control operations.
- Meanwhile, within the **Prosecutor General's Office**, the prosecution units specialising in investigating specific predicate offences and related Money Laundering and terrorist financing offences are:
  - **Special Anti-Drugs Prosecution Service**: for drug trafficking offences and money laundering related to this offence.

- **Special Prosecutor's Office against Corruption and Organised Crime:** for offences relating to corruption (bribery, abuse of office, embezzlement, etc.), organised crime and Money Laundering linked to these offences (excluding drug trafficking or terrorism offences).
- **Prosecutor's Office of the Audiencia Nacional**: for offences of terrorism and Terrorist Financing.
- In the judicial sphere, cases involving Money Laundering offences may be tried, depending on the circumstances and the seriousness of the offences, by the **Provincial Courts, the Audiencia Nacional** and, in exceptional cases, by the **High Courts of Justice** of the Autonomous Communities.

For its part, the Audiencia Nacional has exclusive jurisdiction to hear cases involving Terrorist Financing and Money Laundering offences related to it.

4. MILESTONE ANALYSIS: THE IMPACT OF THE COVID-19 PANDEMIC AND THE WAR BETWEEN RUSSIA AND UKRAINE.

4.1. The impact of the COVID-19 pandemic.

COVID-19 was an international crisis that affected the humanitarian, economic and social spheres alike. In response to the World Health Organisation's declaration of COVID-19 as a pandemic on 20 March 2020, Royal Decree 463/2020 of 14 March was passed in Spain. This Royal Decree declared a state of alarm with the aim of managing and combating the health crisis caused by COVID-19.

In this context, measures were adopted to restrict domestic movement to essential journeys only, leading to the closure of, amongst other things, economic activities, schools and borders. This necessitated the rapid adoption of new technologies and the digitalisation of sectors, businesses and institutions to enable them to continue their operations. The global economy was affected by this crisis and financial crime increased significantly, as reflected in the figures from the Money Laundering and Terrorist Financing Statistical Report, which show that money laundering and terrorist financing alerts rose by 51 per cent, court rulings increased by 19 per cent and convictions rose by 36 per cent when comparing 2021 data with that of 2019. In 2022, the figures for both court rulings and convictions have returned to levels similar to those seen in 2019.

Data on reports of suspicious activity submitted to SEPBLAC show that, amongst the criminal activities reported by regulated entities, property offences saw the most exponential growth, rising from 465 reports of suspicious activity in 2019 to 3,044 in 2022, representing a 555 per cent increase in 2022 compared with 2019.

The study "Financial Digitalisation and COVID-19: Empirical Evidence"[9] analyses financial digitalisation and the implications arising from the COVID-19 pandemic, and confirms the potential use by members of the public of digital channels when interacting with financial institutions and making digital payments, the main cause being the lockdown and social distancing measures put in place during the health crisis.

In the field of Money Laundering and Terrorist Financing (ML/TF), the outcome of the health crisis and the accelerated digitalisation, as mentioned above, has led to an increase in property offences, particularly those related to fraud, cybercrime, identity theft, counterfeiting of medical products, fraud to obtain public funds, tax evasion and donation-related scams.

Furthermore, the economic difficulties faced by the business sector provided an ideal environment for organised crime groups to channel funds of illicit origin into the economy. In addition, there was a reduction in the use of physical cash

[9] Funcas, 2021.

amongst private individuals, which led to an increase in shipments disguised as commercial transactions or goods transport, alongside a rise in bank transfers involving the activities of so-called 'money mules'.

However, the laundering of funds obtained by criminal organisations slowed down during the state of emergency due to the restrictions on domestic movement that were imposed.

One of the main weaknesses of the Spanish supervisory system was the reduction in *on-site* inspections by supervisors, which made it necessary to adapt the supervisory model to the needs of the moment, primarily affecting inspections that were already underway.

In the legal sphere, the transposition of the Fifth Directive into Spanish law was also delayed due to the urgent need to introduce health, economic and social contingency measures to combat the effects of the crisis. However, Royal Decree-Law 7/2021 of 27 April and Law 18/2022 of 28 September, ' ' on the creation and growth of businesses, enabled this transposition to take place.

4.2. The impact of the war between Russia and Ukraine.

In February 2022, Russia launched a war of aggression against Ukraine which continues to this day. The existence of a war on European soil and its consequences paint a picture in which new risks are emerging in relation to Money Laundering and its underlying offences.

In particular, there is a risk that weapons used in the conflict may be diverted for criminal purposes elsewhere in Europe. Consequently, the European Union is assisting Ukraine in putting in place the necessary controls to prevent this.

Furthermore, controls on trade in defence and dual-use equipment must be tightened to ensure that Russia and its allies do not acquire products that could be used for their war effort.

The invasion of Ukraine has led to a significant movement of people fleeing the war. In situations such as this, there is an increased risk that migrants may become victims of crimes related to human trafficking. It is therefore necessary to monitor financial transactions that may be linked to their exploitation.

The movement of people involves the movement of cash, and organised crime may also exploit these movements to transfer money of illegal origin.

International sanctions have been imposed on Russia and Belarus in response to the invasion of Ukraine. The European Union's measures are designed to weaken Russia's economic base, depriving it of vital technologies and markets, and significantly limiting its ability to sustain the war. The sanctions apply to Russia and Belarus and are an extension and expansion of those that had already been in place since 2014, as a result of Russian interference in Ukraine. The sanctions include, amongst others:

- Arms embargoes.
- Restrictions on the entry of individuals included on sanctions lists (travel bans).
- The freezing of assets belonging to individuals or entities included on sanctions lists.
- Economic sanctions or restrictions applicable to certain sectors of economic activity, such as a ban on importing or exporting certain goods, a ban on investment, a ban on providing certain services, etc.

Individual sanctions require the freezing of assets in Europe belonging to certain specifically designated individuals and entities. The freeze affects not only the nominal assets of the sanctioned party, but must also extend to assets under their control. In this regard, the correct identification of beneficial ownership is crucial. In cases where the sanctioned party takes steps to circumvent the sanctions, proving control over their assets can be difficult. Trade

sanctions increase the likelihood of smuggling, by altering the true origin or destination of goods and channelling receipts and payments via third countries.

The ban on payments to the Russian public sector and to Russian companies in certain sectors may lead to the creation or consolidation of mechanisms to offset financial flows arising from trade with Russia, thereby circumventing the direct transfer of funds.

5. MAIN THREATS RELATED TO MONEY LAUNDERING.

When identifying ***threats*** within the context of the fight against Money Laundering/Terrorism Financing, the definition provided by the FATF should be followed: *"those persons, groups of persons or their activities that pose a potential danger due to their capacity to cause harm to the State, society, the economy or other fundamental elements of a country's life"*.

In the specific case of Money Laundering, criminal organisations and their activities constitute threats that exploit vulnerabilities in the system to give the appearance of legality to the illicit financial gains derived from these criminal activities.

The identification of the main threats to Money Laundering activities is carried out through various analyses and contributions from those public institutions responsible for combating this type of organisation and activity.

In Spain, as set out both in the Annual Money Laundering/Terrorism Financing Statistical Report published by the Prevention Commission, containing financial intelligence from SEPBLAC and the LEAs, and in the Ministry of Home Affairs' Crime Statistics System, the main threats in the field of Money Laundering stem from:

(i) Organised crime.
(ii) Drug trafficking.
(iii) Economic and financial crimes, mainly related to fraud and corruption.

In addition to these offences, there are threats related to Money Laundering activities linked to crimes committed in Spain and other countries.

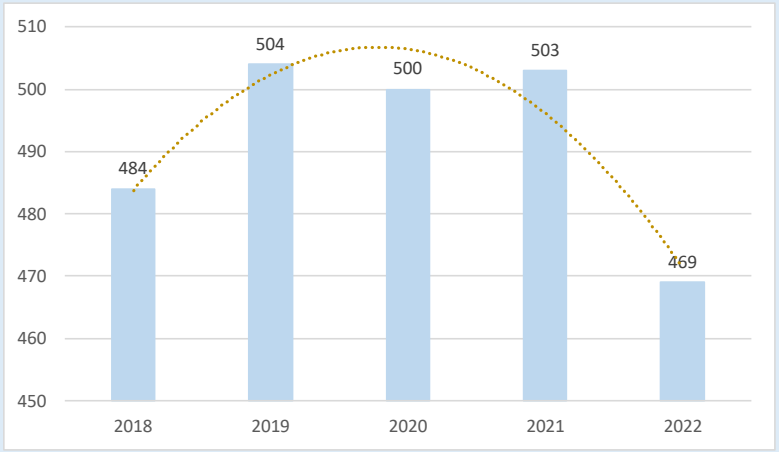
5.1. Organised Crime.

Currently, various analyses identify organised crime as one of the main threats to Spanish security. These include the 2021 National Security Strategy, the National Strategy against Organised Crime and Serious Crime (2019–2023) and the 2022 Annual Security Report.

The conclusions of these studies are reinforced by the statistical data published annually by CITCO and by the crime figures set out in the reports of the Ministry of Home Affairs, which establish that organised crime is a transnational, flexible and opaque phenomenon with an enormous capacity for destabilisation, capable of affecting social, economic and political structures and values.

These characteristics mean that organised crime is becoming increasingly intertwined with illicit activities such as drug trafficking, *ransomware* attacks, human trafficking, tax evasion and terrorism, amongst others. The 2022 National Security Report confirms that specialisation and the creation of synergies and links between criminal organisations to share or facilitate resources are becoming increasingly common.

CUADRO 2. Grupos de crimen organizado con actividad en España 2018-2022



Fuente: Elaboración propia, datos Ministerio del Interior-CITCO

The 2021 National Security Strategy set out the following lines of action for combating organised crime and serious crime: (i) to draw up a strategic plan to combat illicit enrichment by criminal organisations and offenders; and (ii) to develop a specific national strategic plan against human trafficking and exploitation.

As part of the implementation of these lines of action, the National Security Council approved the *"National Strategic Plan against Trafficking in and Exploitation of Human Beings 2021–2023 – PENTRA"* in November 2021. Furthermore, in February 2024, the *"Strategic Plan to Combat the Illicit Enrichment of Criminal Organisations and Offenders* – PELCEIL" was presented. Both plans are coordinated by CITCO, with the participation of other authorities[10] , and are designed to enhance the effectiveness and operational capacity of the various preventive measures established in each area, to promote new actions in areas not previously addressed – in the case of PENTRA – and to optimise efforts to recover illicit assets.

A proliferation of activities linked to organised crime has been detected, some of which have emerged as a result of new technologies and others which have evolved through the use of these technologies. Among the operations detected in connection with organised crime is the use of *clandestine banking* systems *(underground banking*). This activity has given rise to a new and complex financial ecosystem, created and managed by criminal organisations to facilitate their criminal activity and profit from it. Criminal organisations, particularly those operating internationally and possessing significant financial resources, have expanded the provision of underground banking systems—a criminal activity in its own right—serving numerous criminal organisations of various kinds.

This underground financial system is controlled by professionals who use various known money-laundering techniques to move funds. Among the methods used in the underground financial ecosystem are traditional cash-to-cash settlement schemes such as *hawala*, in which not only are cash-to-cash transactions carried out, but an increasing number of cash-to-crypto-asset (CA) or CA-to-cash transactions are also being detected. This combination speeds up the movement of funds globally and makes it even more difficult to trace these movements.

Furthermore, this underground system is also intertwined with money laundering operations carried out through international trade transactions (*trade-based money laundering*), in which legitimate and illicit cash flows are intermingled, and genuine transactions are combined with large-scale fictitious import and export operations. This

[10] LEAs, various Ministries (Equality, Inclusion, Social Security and Migration; Labour and the Social Economy; Justice; Social Rights and the 2030 Agenda; Education and Foreign Affairs; Economy, Trade and Industry), the General Council of the Judiciary, the Prosecutor General's Office and the Spanish Network Against Trafficking in Human Beings.

commercial scheme utilises both the official and clandestine financial systems, serving to disguise money-laundering operations and/or finance large-scale criminal activities.

The criminal phenomenon of underground banking systems is a widespread reality in the economy, one which is very difficult to quantify, given the lack of evidence that would enable their identification and prosecution by the police.

The 2022 National Security Report highlights drug trafficking as the most significant manifestation of organised crime. However, this document highlights the evolution of this criminal activity, encompassing the existence of multi-criminal groups; the emergence and development of the 'gang' phenomenon (violent youth groups); and the activities in Spain of new international groups with their headquarters or leaders based in other countries (the Netherlands, the Gulf States, the United Kingdom, etc.). This international activity, which creates synergies between international criminal groups, has facilitated the emergence of complex criminal platforms and structures with support in different countries, making it difficult to investigate and dismantle them.

In the economic sphere, cybercrime-related offences have seen the greatest growth, with computer fraud being the most prevalent activity in this area, facilitated by the use of cryptocurrency and virtual currencies alongside techniques that obscure their traceability in order to conceal their illicit origin.

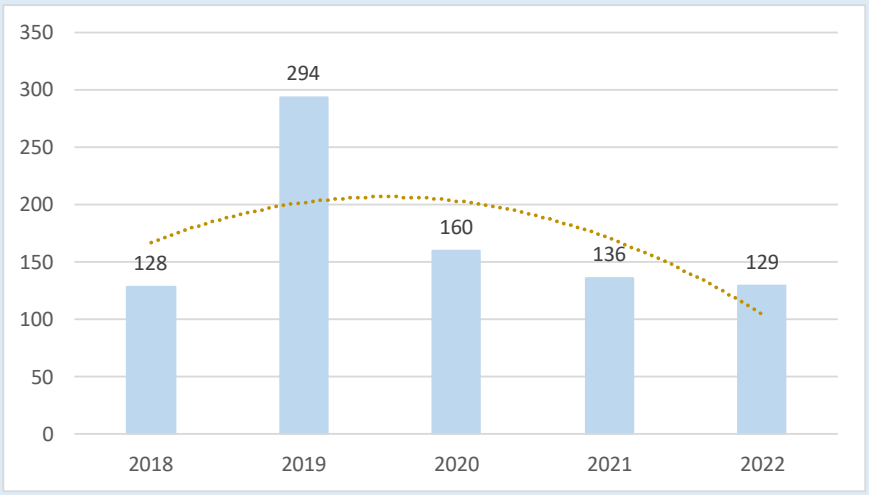
The Ministry of Home Affairs' response to combating these cybercrimes is primarily structured around the Strategic Plan against Cybercrime (PECC), which focuses on prevention and utilises the promotion of collaboration between the various LEAs and legal practitioners as a key tool.

From an economic perspective, it must not be forgotten that organised crime, operating under the guise of legitimate business, has the ultimate aim of generating substantial financial gains, generally within complex structures involving companies set up for criminal purposes or others whose activities are lawful but which are used as a means of channelling funds.[11] .

In the social sphere, organised crime takes on particular significance when it involves actions related to human trafficking, such as the exploitation of women, children who are victims of the production and distribution of child sexual abuse material, or the trafficking and exploitation of people in general. This phenomenon not only poses a threat to national security but also constitutes a serious violation of human rights, requiring measures that promote prevention through the effective prosecution of acts of exploitation arising from human trafficking offences and the prosecution and criminal punishment of the individuals involved, without neglecting the protection and care of the victims who have been trafficked.

[11] https://www.guardiacivil.es/ga/prensa/noticias/8398.html
First operation by the European Public Prosecutor's Office in Spain involving arrests, targeting a VAT fraud ring (elperiodico.com).

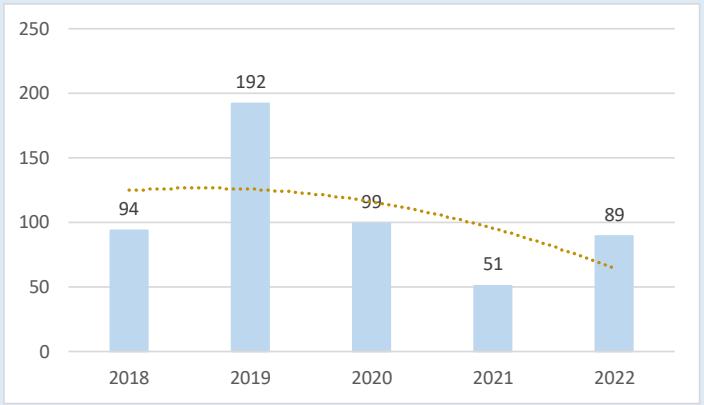
CUADRO 3. Víctimas de trata sexual 2018-2022



Fuente: Elaboración propia, datos Ministerio del Interior-CITCO

Table 3 shows that the number of victims of sex trafficking has fallen in 2022 compared with 2021, according to data from the Ministry of Home Affairs. The number of people identified as victims of labour trafficking (Table 4) continues to follow the same trend as in 2020.

Cuadro 4. Víctimas por trata laboral 2018-2022



Fuente: Elaboración propia, datos Ministerio del Interior-CITCO

The war in Ukraine has heightened the threats relating to human trafficking for the purposes of sexual and labour exploitation in Europe. However, in Spain, no major changes have been identified with regard to serious and organised crime activities linked to or arising from the war in Ukraine.

Following the implementation of the EU's restrictive measures against Russia, there has been an increase, on the one hand, in the threat of illicit funds entering the country via clandestine financial systems, frontmen and intermediaries to circumvent the administrative sanctions imposed, and, on the other hand, in the trafficking of weapons from the war by organised groups.

In short, organised crime is a dynamic, constantly evolving phenomenon with a great capacity to adapt in order to obtain illicit profits; this inherently involves the commission of other criminal activities such as drug trafficking, illicit trade, terrorism, fraud, cybercrime and criminal violence, and operates on a supranational scale. This nature makes it a global threat, where the development of new technologies, the entry into the financial system of new actors through whom funds can be channelled, and the increasingly digital nature of society's operations—accelerated by the COVID-

19 pandemic—exacerbate the damage it can cause to the system, affecting society, the economy, and national and international security.

In the fight against the harm associated with organised crime, international and national cooperation amongst the various LEAs is a decisive factor . In Spain, during 2022, 93 per cent of the groups detected were either fully or partially dismantled. Furthermore, 61 per cent of the groups were involved in international activity. Among the groups linked to **drug trafficking networks,** the most significant are:

a) **Groups involved in drug trafficking from Latin America**, operating in Spain in cooperation with local networks that facilitate the smuggling and distribution of drugs. In these cases, there is a direct link between the predicate offence and Money Laundering activity. These groups operating in Spain smuggle drugs into Europe mainly via pre-established routes through our country. The funds they generate are channelled into the financial system via networks of individuals and entities, including companies involved in the trade of goods and services, which allows them to justify their transfers and income through various means (alleged commercial transactions, cash receipts, drug couriers or remittances, amongst other methods).

b) **Groups involved in drug trafficking from the Maghreb,** which, as in the previous case, operate in Spain in cooperation with local networks that facilitate the smuggling and distribution of drugs. Spain is, by far, the EU country with the highest volume of cannabis trafficking, as analysed in the following section. Due to its geographical proximity, these organised groups use Spain primarily as a transit route to other European destinations, in coordination with local criminal groups, which has created a serious security situation that particularly affects the Campo de Gibraltar area. This illegal trafficking generates vast amounts of cash, with frequent cash-in-transit operations, money mules and transactions into the financial system disguised as commercial operations.

c) Groups linked to **tax fraud associated with commercial activities**, mainly through companies involved in the production and wholesale distribution of goods manufactured abroad and their sale through the retail network throughout the country. These groups, mainly of Chinese and East Asian origin, manage to generate enormous sums of money in breach of tax regulations, which they either send abroad (either in cash, making significant use of human couriers, or via transfers disguised as commercial transactions) or invest in Spain, primarily through the purchase of commercial premises. These money-laundering activities, stemming from tax offences, also sometimes conceal other predicate offences such as sexual offences, breaches of workers' rights, illegal drug trafficking or illegal gambling, amongst others.

d) Groups specialising in **property offences**, burglaries of business premises and homes, the illicit trafficking of vehicles, and other violent offences against banks and establishments holding high-value goods such as jewellery and art. These are generally groups of foreign origin, mainly from Eastern Europe and Western Asia, in some cases itinerant, who do not always have a permanent residence in Spain. Due to the very nature of the offences committed and the measures in place within the economic system itself, it is difficult for the proceeds to be integrated into the Spanish financial system; consequently, they are frequently transferred to other territories – sometimes outside the European Union – where they are deposited in financial institutions, offered for sale, and so on.

e) Groups specialising in the **fraudulent use of payment methods,** particularly credit and debit cards. The weaknesses in the system and the number of fraud cases have led card-issuing organisations to develop complex systems to ensure the security of users, who are exposed to theft and the illegal copying of data. The groups committing these offences operate across all EU countries, distinguishing between the territories where cardholders reside, where data is captured, and where fraudulent use takes place. The proliferation of online platforms where users can purchase goods and services, place bets or participate in games of chance, etc., has introduced a factor that greatly facilitates the laundering of proceeds from these crimes.

f) Groups specialising in **large-scale online fraud**. For several years now, organisations specialising in the fight against crime have been warning of a highly specialised criminal network engaged in large-scale fraud, mainly originating in West Africa, through the sending of *the* original *'Nigerian* letters', in which messages (by post, telephone, email, etc.) are sent to potential victims in order to obtain funds. Links between these groups and other offences (including those relating to sexual exploitation) have also been established. Financial transactions involving the funds sent by victims are rapidly transferred via various systems, including the use of payment service providers and bank accounts opened under false identities or for fraudulent purposes.

g) Groups that **carry out criminal activities in other jurisdictions but bring illicit funds into Spain**. This is a form of crime which, in Spain, generally does not involve specific criminal acts but involves Money Laundering operations through the purchase of luxury goods and property. Of particular note is the presence of groups from other European countries where they commit offences relating to corruption, extortion and illicit trafficking; these groups seek to establish Spain as the location for investment or the purchase of residences for some of their leaders and members, sometimes through complex money-laundering schemes. These groups launder their illicit proceeds through complex corporate and commercial transactions, utilising commercial companies registered in various jurisdictions – some of them in EU countries – with the initial banking transactions taking place in countries across all continents, including, in some cases, EU countries.

h) Groups linked to **political or financial corruption schemes**, both national and international. Generally speaking, these groups engage in activities with repercussions across several countries, such that the country in which the criminal act through which the corruption (misappropriation of funds, bribery, fraud, etc.) or the corresponding financial offence is committed is different from the country of residence of the perpetrators, and also different from the country in which the funds are received or the assets – predominantly property – are acquired.

Spanish groups involved in such activities carry out their criminal acts in our country, generally in connection with urban development and public services projects, and use foreign countries to hold accounts and deposits and to register the commercial companies in whose name these accounts are held.

For their part, **foreign groups** linked to these corruption offences choose Spain as one of the countries to which to channel funds, through complex international transfer schemes involving two or more countries, and subsequently use these funds to purchase assets, generally luxury property in tourist areas, but also in more affluent neighbourhoods of major cities.

The methods used by these groups to channel funds are highly diverse, ranging from the use of clandestine banking systems – where the presence of CA has been identified – to channelling funds through the art and antiques market, given the nature of these assets, which depreciate little or not at all.

5.2. Drug trafficking[12] .

Drug trafficking in Spain is linked to the European landscape, where there is evidence of an increase in the consumption and availability of drugs within society.

Spain's circumstances, climate and geography mean that it is traditionally regarded as a country of transit and drug consumption.

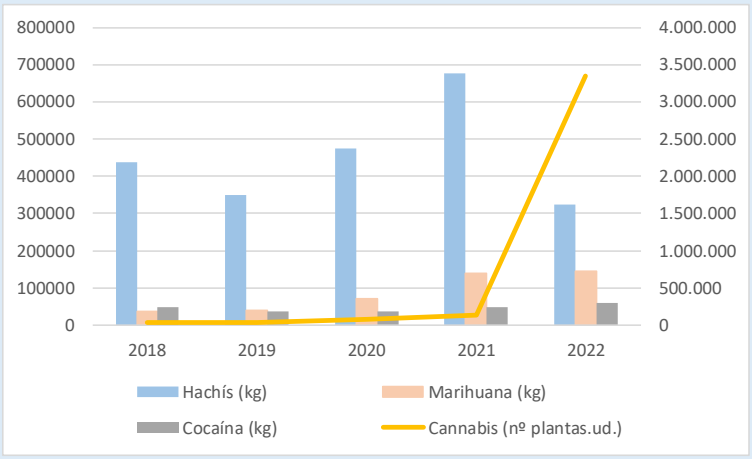
Although the most prevalent substances are hashish and cocaine, the 2023 Annual Report of the Office of the Prosecutor General highlights as alarming the normalisation of the use of substances such as cannabis and Spain's current role, given that it has become the leading producer of cannabis in the EU.

[12] Prosecutor General Annual Report 2023. Section on the Special Anti-Drugs Prosecutor's Office.

This status as a producing country poses a risk of increased consumption and encourages foreign criminal organisations to establish a presence in Spain. It is this reality that is currently requiring greater efforts in police investigations, as drug trafficking can be linked to other criminal activities such as organised crime, human trafficking, tax evasion and arms trafficking. The LEAs, based on their investigations, confirm the use of a range of drugs characterised by the fact that they are not covered by international control conventions; and although the figures are not yet alarming, their use is accelerating, particularly due to online advertising. These are known as New Psychoactive Substances (NPS).

As regards seizures, according to data from the 2023 Report on Alcohol, Drugs and Tobacco, more than 389 tonnes were seized in 2022. Table 5 shows the trend in drugs seized.

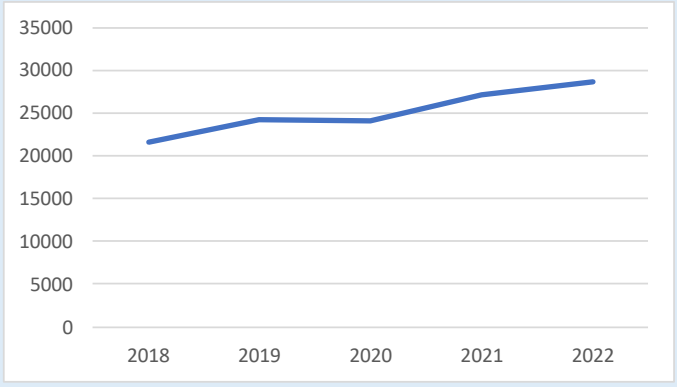
CUADRO 5. Evolución de la droga incautada en España 2018-2022



Fuente: Elaboración propia, datos Ministerio del Interior-CITCO

In 2022, 28,678 arrests were made for drug trafficking offences. Table 6 illustrates the upward trend in the number of arrests, which reached its highest level in 2022.

CUADRO 6 Detenciones por tráfico de drogas (2018-2022)



Fuente: Observatorio español de las drogas y Adicciones

55.7 per cent of arrests were for cannabis trafficking, followed by cocaine trafficking (23.5 per cent), amphetamine-type drugs (9.8 per cent) and opiates (4.6 per cent).

According to the National Anti-Drugs Plan Office, the consumption data regularly provided by the Spanish Observatory on Drugs and Drug Addiction show that the percentage of people who have used cannabis and cocaine has increased since 2020, whilst the figures for other substances remain at similar levels.

The total number of cases handled by the Special Anti-Drug Prosecutor's Office relating to drug trafficking in 2022 stood at 21,740, representing an increase of more than 20 per cent since 2018; in these cases, despite the difficulty in identifying the predicate offence, Money Laundering is considered to be a cross-cutting issue in this type of criminal activity. Alongside Madrid (3,029 cases, representing a 13.74 per cent increase in 2022), the provinces of Seville and Las Palmas de Gran Canaria stand out, showing increases of 17 per cent and 38 per cent, respectively, since 2021.

As regards those convicted of drug trafficking by the Audiencia Nacional in 2022, the data show that, of the 29 public health-related judgements handed down by the Criminal Chamber of the Audiencia Nacional, 64 Spanish nationals, 59 foreign nationals and one legal entity were convicted.

The 2022 National Security Report notes that the Strait of Gibraltar and the Alboran Sea are sensitive areas in relation to drug trafficking. In order to combat this threat, the LEAs are involved in various operations requiring both domestic cooperation amongst themselves and international cooperation with other foreign authorities[13] .

The Crime Statistics Report for the fourth quarter of 2022 shows a 14.4 per cent increase in drug trafficking offences in 2022 compared with 2019 and a 3.8 per cent increase compared with 2021, attributing this rise to the actions of the LEAs, as part of specific plans such as the Special Security Plan for the Campo de Gibraltar; in reality, this is an indicator of police activity in tackling this type of crime.

The Special Security Plan for the Campo de Gibraltar has been extended until 2025, marking the fourth such extension. During its third extension (valid until 31 December 2023), its area of operation was expanded to cover three Andalusian provinces, encompassing the entire southern Spanish coast.

5.3. Economic and financial crimes: fraud, tax offences, and cases linked to corruption .

The 2022 National Security Report identifies economic and financial crime as the main threat to Spain's economic and financial stability. This assessment is based on the harmful effects they cause, such as: a fall in productivity rates; the diversion of funds originally earmarked for public policy initiatives; disruption to the socio-economic order; and a loss of legitimacy on the part of public authorities, which undermines public confidence and damages the country's credibility and reputation.

In 2022, reports of suspicious transactions relating to fraud increased by 554 per cent compared with 2019, followed by those linked to offences against the Treasury. Property offences associated with fraud and offences involving VAT fraud account for 43 per cent of the offences identified in reports based on circumstantial evidence submitted by regulated entities in 2022.

The progressive digitalisation of society and, in particular, advances in communications systems, the development of social media and the widespread adoption of online commerce have opened up new possibilities for fraud committed via technological means (cyberfraud or cyber-attacks).

[13] Examples of these include: Customs Surveillance participates in Operation PASCAL; at national level, there is collaboration in the ORION Naval Campaign; the Policía Nacional and the Guardia Civil are involved in the "Port Cooperation Project"; between July and September 2022, the Guardia Civil carried out 'Operation Safe Ports', whilst Maritime Rescue closely monitors the sea using aircraft and satellites to enhance maritime safety.

Much of this technology-enabled fraud is carried out by international organised crime groups which divide the various stages of the fraud process – including the laundering of the proceeds – amongst highly specialised sub-groups. Generally, these stages take place in different countries, which makes investigation and prosecution more difficult. The capacity of these groups is such that the phenomenon has come to be described as *the 'industrialisation of fraud*'.

Cyberfraud is a global threat that causes individual harm to directly affected people and organisations and undermines public confidence in new technologies, the economy, the financial system and institutions.

This global nature is evident in the activities carried out by organised crime groups involved in fraud, which, in order to launder the funds obtained through their criminal activity, need to ensure that the funds of fraud victims become untraceable. Typically, this type of money laundering involves international fund transfers, the conversion of foreign currency into cash and, more recently, conversion into CA.

Among the methods used to carry out Money Laundering stemming from cyberfraud is the use of bank accounts to collect, directly or indirectly, funds from victims and then, in the majority of cases, transfer them to other countries. The operations observed in these accounts can vary. Incoming payments may originate from the victims of fraud or from other intermediary accounts and are generally made via bank transfers. The most common outflows are international transfers and cash withdrawals (mainly abroad). In recent years, the purchase of CA has been the destination for a large proportion of the defrauded funds. Furthermore, the funds may be laundered through international trade transactions, being used to pay for exports (in cash or by transfer) and then settled with importers in the countries to which the exported goods are destined.

With the aim of curbing tax fraud, Law 11/2021 of 9 July on measures to prevent and combat tax fraud came into force, transposing Directive (EU) 2016/1164 of 12 July 2016, which lays down rules against tax avoidance practices that directly affect the functioning of the internal market, and amending various tax provisions and regulations governing gambling. This Law amended the aforementioned Article 7 of Law 7/2012 of 29 October, reducing the general limit on cash payments from 2,500 to 1,000 euros and, in the case of private individuals with tax residence outside Spain, from 15,000 to 10,000 euros.

TABLE 7. Types of fraud

Social Security fraud: there are various forms of Social Security fraud, which may consist of the non-payment of contributions due on behalf of employees, or the receipt of benefits or public assistance on non-existent grounds. This type of fraudulent activity has a detrimental impact on unfair competition; the black economy; corruption; workers' rights; and the development of conduct associated with human trafficking for labour exploitation, amongst other issues.

Influence peddling, embezzlement, perversion of justice and bribery (proper and improper): these are offences linked to corrupt practices that are usually related to decisions by public authorities to award certain private entities the right to carry out public activities through contracts, concessions, licences, etc., in many cases relating to public services, public works or planning permissions. These decisions may involve the issuing of false invoices; financial or material benefits for the awarding authority; or the awarding of contracts to entities indirectly controlled by the awarding authority itself, thereby enabling the automatic legitimisation of the profits obtained from the criminal activity.

Tax fraud: alongside traditional tax offences involving the non-payment of taxes to the tax authorities (income, wealth, corporation tax), figures for criminal activities relating to VAT fraud remain high, whether through evading payment or via the fraudulent claiming of VAT refunds by national authorities following a chain of transactions (so-

called ‘carousel’ schemes). In recent years, the AEAT has allocated a considerable amount of resources to prosecuting such conduct through the courts, and these resources are increasing every year.

Customs fraud: the most significant criminal activity involves the importation of goods by undervaluing both the quantities of goods traded and the values declared to customs, thereby defrauding the EU Treasury of import duties (tariffs). Such fraud is particularly prevalent in relation to products imported from Asia. Criminal groups use various schemes to avoid paying taxes and generate substantial profits by selling these products (whether genuine or counterfeit) at prices lower than their market equivalents, thereby creating situations of unfair competition. The scale and number of operations carried out by the AEAT in recent years have highlighted the existence of significant organised crime operations and networks involved in these activities. Other significant forms of fraud relate to the origin or tariff classification of goods, as well as the abuse of certain schemes such as the non-customs warehouse scheme and Scheme 42 (obtaining VAT exemption when imported goods are dispatched to another EU Member State).

Corporate offences: these involve a wide range of conduct carried out by company directors or executives who, in order to achieve certain personal ends, engage in market activities to the detriment of the company itself, its shareholders or third parties. In many cases, they are linked to offences involving the falsification of corporate documents.

Fraud involving public subsidies: this involves the improper obtaining of public funds by falsifying the conditions required for their award, concealing circumstances that would have prevented their award, or failing to comply with the conditions or purposes for which the subsidy was granted.

Investment fraud: this involves frauds in which deception is used to persuade the victim to invest money in investment products that are not regulated by the CNMV, or in CA (a form of fraud that has become more prevalent in recent years). These schemes may be carried out by individuals or companies (so-called ‘financial fly-by-night operators’) without being authorised to operate in the securities markets or to provide investment services as provided for in the Securities Law. Victims are approached by telephone or via a website and are defrauded when they make bank transfers – sometimes involving sums running into millions – to the bank accounts they are instructed to use. There are three main types: ‘*boiler* rooms’, Ponzi schemes and pyramid schemes.

5.4. Money Laundering by third parties and arising from offences committed abroad .

The transnational nature of financial transactions in a system as globalised as today’s is a clear fact. Investigations carried out by various national authorities demonstrate the existence of organised crime groups that are interconnected across multiple countries, facilitating Money Laundering in Spain (as in other countries) of funds derived from criminal activities committed abroad, regardless of whether the predicate offence has any connection with our country.

Within this framework, law enforcement agencies have uncovered operations with national and international links, connected to the buying and selling of luxury goods and works of art, and to the Spanish property market.

The buying and selling of luxury goods is a particularly attractive activity for Money Laundering, given that, by their very nature, such items not only accumulate significant value but also retain it over time; this enables criminal organisations to recoup their initial investment following their sale, and even to make further profits.

Furthermore, the Spanish property market is highly attractive to organised crime, given its economic characteristics and the country's status as a tourist destination. With regard to the potential benefits for Money Laundering, the following aspects are particularly noteworthy:

- It is a sector traditionally linked to activities involving the generation and concealment of funds of illicit fiscal origin.
- Ownership of immovable property can take many different legal forms, both national and international, including forms of temporary or spatial co-ownership.
- The valuation of property is highly subjective, linked to factors not directly derived from the property itself.
- It is a sector highly susceptible to criminal behaviour linked to corruption.

With regard to investment in real estate, account must be taken of the money-laundering risks posed by citizenship-by-investment schemes (Golden Passport) and residence-by-investment schemes (Golden Visa), which grant citizenship or residence to third-country nationals in exchange for primarily financial considerations. In Spain, 'Golden Passports' are not provided for; however, 'Golden Visas' are. Law 14/2013 of 27 September on Support for Entrepreneurs and their Internationalisation regulates a residence visa for investors and a residence permit for investors.

The residence visa for investors is aimed at non-resident foreign nationals who intend to enter Spanish territory with the aim of making a significant capital investment. This visa must be applied for by interested investors.

According to data provided by the Ministry of Inclusion, Social Security and Migration to *Transparency International Spain*[14] regarding investor visas granted from 1 January 2017 to 31 March 2022, it can be seen that a total of 6,200 visas have been granted to investors of all nationalities, of which 96.18 per cent were granted on the basis of the purchase of property .

From the Money Laundering perspective, the risks associated with this type of scheme are linked to corruption, tax evasion, organised crime, the circumvention of international financial sanctions, and cross-border movements of funds.

Despite these risks, it is worth noting that carrying out this type of property investment requires the involvement, at a minimum, of notaries, land registrars and financial institutions. These regulated entities comply with the policies and procedures set out in Law 10/2010 of 28 April, and also have powerful databases to identify the beneficial ownership of such investments and ensure compliance with due diligence measures.

6. MAIN THREATS OF TERRORIST FINANCING[15] .

Terrorism remains a national and international threat, as developments in the financial system and new technologies create new opportunities for terrorist organisations to finance and channel funds.

[14] https://transparencia.org.es/estudios-y-publicaciones/la-adquisicion-de-la-residencia-en-espana-a-traves-de-golden-visas-principales-riesgos-y-desafios/

[15] Sources: "National Security Report 2022", "FGE Annual Report 2023. Public Prosecutor's Office of Audiencia Nacional", "The Fight against ETA and International Terrorism" – 12th Parliament. Ministry of Home Affairs.

The ability of these terrorist groups to adapt to the preventive barriers put in place by the LEAs highlights the need to identify and neutralise sources of funding.

Jihadist terrorism has gained strength in Africa, particularly in the Sahel, the Lake Chad basin and the Horn of Africa.

The terrorism that persists in Spain currently exhibits more complex and diverse characteristics, with jihadist terrorism posing the greatest national threat through its two main groups, Daesh and Al-Qaeda, both of which maintain a particularly active presence in Africa. The 2022 National Security Report assesses the possibility of terrorist attacks being carried out by 'lone wolves'[16] .

This term encompasses the main threats posed by jihadist activity in Spain, which are, on the one hand, the existence of individual actors and independent cells and, on the other, the phenomenon of *'homegrown terrorist fighters'* (hereinafter HTFs) – individuals radicalised in European countries, including Spain, who issue terrorist calls via the internet.

Furthermore, in Spain, in addition to these individual actions, there is a prevalence of logistical networks providing financial support – primarily to Daesh – and, above all, cells dedicated to the recruitment, indoctrination and enlistment of followers, in both physical and virtual environments.

In this context, new technologies play a significant role in the dissemination of violent and extremist ideas by terrorists, with the aim of attracting and recruiting individuals via social media, online platforms or gaming chat rooms. The latter channel is one of the means used by terrorists to communicate, radicalise and recruit without revealing the true purpose of the message, as terrorist propaganda can be concealed within the content of games. Within this framework, the use of artificial intelligence to obtain financial resources for terrorist financing is highlighted. With regard to new trends in carrying out terrorist activities, the potential use by terrorist groups of remotely piloted aerial vehicles—which can be configured as weapons for carrying out terrorist attacks—is identified as a threat to national security.

Furthermore, as noted in the 2020 NRA, domestic terrorist organisations linked to the Basque independence movement (ETA) and the Marxist-Leninist armed movement (GRAPO) have either disappeared or are in the process of doing so. In this regard, activities linked to ETA, which are increasingly marginal, focus on demanding unconditional amnesty for all ETA prisoners, as well as the return of those in exile.

With regard to investigations by the LEAs, 100 police investigations were carried out in 2022. In the judicial sphere, 163 preliminary proceedings were conducted on terrorism charges, resulting in 11 convictions and 25 individuals sentenced by the Criminal Division.

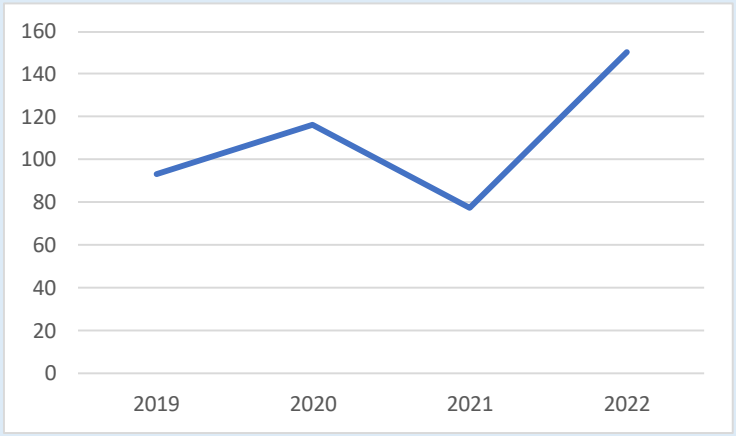
As for domestic terrorism, although activity linked to ETA is minimal, several police operations were carried out in 2022, leading to 55 arrests, mainly for public disorder, with the province of Álava being the main focus of these operations.

Furthermore, according to the 2023 Annual Report of the Audiencia Nacional Public Prosecutor's Office Special Unit, jihadist terrorism continues to show an upward trend in terms of preliminary investigations initiated, with 132 cases recorded for 2022, accounting for 81 per cent of the total number of cases opened on terrorism charges.

As regards the total figures for those arrested and prosecuted for activities linked to terrorism, Table 8 shows that the trend is rising, with a 94 per cent increase in arrests compared with 2019.

[16] A person who carries out a terrorist act without being directly linked to a leader or receiving support from an organisation or group.

CUADRO 8. Detenciones por actividades vinculadas al terrorismo



Fuente: Memoria de la Fiscalía de la Audiencia Nacional 2023

Counter-terrorism activity targeting jihadism in Spain resulted in 17 police investigations in 2022, leading to 36 arrests, as well as joint operations with Morocco, Austria and Switzerland, which resulted in a further four arrests following the exchange of information with third countries.

6.1. Jihadist terrorism .

Jihadist terrorism has established itself as a permanent threat with a global reach. Terrorist attacks on European soil have been a constant feature over the last decade, driven by the emergence of Daesh and fuelled by a range of internal and external factors, such as the Palestinian-Israeli conflict that began with the Hamas attack on 7 October 2023. Daesh remains the primary threat, having become the benchmark for jihadist terrorism due to its operational capacity, resources, media presence and rapid expansion.

However, these groups are characterised by their rapid adaptability and their ability to adjust to the changes and strategies employed against them. Indiscriminate attacks on crowded places, transport systems or critical infrastructure represent a current trend in jihadist terrorism, which operates both through organised cells and individually, with the aim of causing the greatest number of casualties and achieving a strong propaganda impact.

The activities carried out by members of jihadist terrorist networks dismantled in Spain have mainly involved recruitment, indoctrination and the dispatch of activists to conflict zones. Similarly, arrests have been made in connection with involvement in terrorist networks, logistical support, acts of glorifying terrorism and serious threats for terrorist purposes, as well as the prosecution of individual terrorist activity. The internet and social media are investigated, analysed and prosecuted when used as a virtual terrorist space or as a means of communication.

Therefore, the main elements and activities related to jihadist threats that must be addressed are:

- Currently, the main threat vector is associated with **terrorists or autonomous cells** capable of carrying out, when the opportunity arises and using means that are not particularly sophisticated but highly lethal, attacks against targets repeatedly highlighted in jihadist propaganda or previously attacked in the West (large gatherings of people, tourist sites, military and police personnel, or places of worship of various religious denominations). However, organised attacks by structured cells linked to Daesh cannot be ruled out.

- **Terrorist fighters returning** from theatres such as Syria and Iraq, having gained knowledge and experience in the use of weapons, established contacts and acquired knowledge of routes and facilitators, also act as

catalysts both ideologically and operationally. The process of sending fighters to conflict zones is carried out through national and international networks, which has led to residents of Spain travelling to Syria and Iraq; activities to finance their travel and stay in those areas have been detected.

- Radicalisation, **recruitment and indoctrination** for terrorist purposes are also among the threats that have come to the fore in recent years. This is not only due to the ideologies underpinning them, but also because they constitute the preliminary stage before individuals involved in these processes ultimately join terrorist groups and organisations.

- **Technological developments** have also broadened access to resources available to terrorist groups, increasing their capacity for **financing, recruitment, training, propaganda and glorification**. Against a backdrop of widespread use of social media, the risks of the dissemination of terrorist propaganda and of forms of radicalisation and violent extremism are growing. The internet has been the most effective tool for jihadist propaganda and recruitment. The idea of 'global jihad' has taken shape for thousands of sympathisers or followers through messages that distort reality, with an epic glorification of jihadist fighters. Videos convey messages emphasising the need to embrace violence to combat injustice and the West's lack of understanding.

- Due to its **geographical location** within the European continent, Spain is more vulnerable to certain terrorist groups. Its proximity to the Maghreb – given the intense terrorist and counter-terrorist activity in the countries that make up the region – makes it a focal point for jihadist terrorism, which can exploit the high volume of passenger traffic to infiltrate terrorist elements into Spain and the rest of Europe.

Spain is committed to the fight against terrorism through a response based on a comprehensive model that draws on its experience and coordinates action with its allies, within international initiatives and, in particular, with the EU. The various actors involved in counter-terrorism efforts are drawing on past experience and maintaining constant preparedness in the present. Global terrorism, such as jihadist terrorism, requires a high degree of international cooperation, yet at the same time it manifests local characteristics that make it a form of local terrorism; this necessitates closely coordinated work between the LEAs (Policía Nacional and Guardia Civil), the Mossos d'Esquadra and Ertzaintza police forces, CITCO, the CNI and SEPBLAC.

Spain has developed, as a result of democratic consensus, a comprehensive regulatory framework containing effective investigative tools, as well as a new definition of activities considered to be terrorist in nature, encompassing those preliminary stages of ideological transformation without which violent action would not occur.

Work over recent years has been ongoing on all these fronts: analysing the jihadist phenomenon from new angles and using new methodologies; studying new criminal offences and adapting them to the jihadist reality; analysing intelligence and crimin , contextualising the phenomenon of Daesh terrorism; addressing the issues surrounding minors and returnees from conflict zones; and studying the ideological reorientation of those who have been recruited and indoctrinated.

6.2. Terrorist Financing.

Spain, given its experience in the fight against terrorism, is fully aware of the need to cut off sources of funding and to identify and mitigate vulnerabilities in the system through which funds—whether of lawful or unlawful origin—are channelled for terrorist purposes or to support such purposes in any form.

In the case of jihadist terrorism, the financing and economic needs of terrorist groups have evolved substantially since the attacks of 11 September 2001, when there were significant movements of funds through the international financial system. Currently, the most recent attacks in Europe – the majority of which have involved minimal planning and posed little difficulty – have required little financial backing for their execution for two fundamental reasons: firstly, due to the low material cost of the attacks, many of which have been limited to the use of bladed weapons or vehicles; and secondly, due to the absence of permanent structures requiring resources for their sustained operation.

Following the investigations launched, it has become clear that the main purposes of the funding obtained are the purchase of airline tickets for cell members, the acquisition of computer equipment, the rental of premises, or the group's own upkeep in our country. The same applies to the use to which these funds are put. In previous years, these funds were intended to support the terrorist group itself or some of its members, whereas at present there is a strong focus on the indirect support of that terrorist group, particularly in relation to detention camps, especially Al-Hol and Al-Roj.

With regard to the financing of travel by terrorist fighters who have travelled to join international groups, primarily Daesh, various methods and types of fundraising have been identified, both legal and illegal, carried out either by the terrorists themselves, their associates or supporting organisations.

The methods used to channel funds are varied, including *crowdfunding* and *clandestine banking methods*. Furthermore, it has come to light that *neobanks* are being used which accept deposits in cryptocurrencies and internally convert them into *fiat* currency in order to move funds whilst bypassing traditional banks.

Furthermore, the use of **international remittances** has been detected as a means for families displaced from Europe to Syria and Iraq to send funds to them on a regular basis; these transfers are made in small amounts and often via predetermined and highly specific methods, involving third countries and intermediaries, which makes them difficult to detect.

6.3. ETA terrorism.

ETA has maintained the "cessation of its armed activity" announced in October 2011 and, consequently, has not carried out any attacks. Its dissolution as an organisation was announced in spring 2018. The LEAs have also confirmed that the terrorist group's traditional funding systems, particularly through extortion by means of the so-called 'revolutionary tax', have ceased.

Some dissident groups were involved in low-intensity acts of violence, such as sabotage, graffiti and the display of posters, following the declaration of the 'cessation of activities', in an attempt to gain greater support amongst Basque nationalist activists for campaigns or events in support of and in solidarity with prisoners. Likewise, some individuals linked to these sectors have carried out violent and sabotage-related acts confined to the Basque Country and Navarre, and their evolution and development must be subject to appropriate monitoring and oversight. However, the capacity for mobilisation demonstrated and the danger they pose have not, for the time being, constituted a significant threat, although their evolution and development must be subject to appropriate monitoring and oversight.

With regard to their **funding mechanisms**, it should be noted that, following the cessation of terrorist activity, the extortion of individuals and legal entities—which had traditionally been a significant source of income for the terrorist group—has also come to an end.

6.4. Other terrorist groups.

In recent years, the terrorist organisation PCE(r)-GRAPO has remained in a weakened state, committing no terrorist acts and limiting its activities to proselytising and recruitment within anarchist and radical left-wing circles. Despite this situation, it has never publicly renounced armed struggle or its revolutionary principles, which are incompatible with current legislation.

Meanwhile, some terrorism-related activity linked to Catalan independence movements has recently been detected and is being monitored by the relevant authorities.

With regard to violent activity carried out by individuals or groups of anarchist ideology, this remains at a low and contained level in Spain, although it is worth noting the impact in our country of international campaigns organised via various anarchist websites.

Police action in response to the resurgence of violent activity during the early years of this decade has clearly influenced the current situation, in which recorded acts of violence are limited to attacks and acts of sabotage against the traditional targets declared by the group, as well as to provoking disturbances and clashes with police units during certain rallies and demonstrations.

6.5. National Counter-Terrorism Strategy.

The 2019 National Counter-Terrorism Strategy (ENCOT) was approved by the National Security Council to replace the previous Comprehensive Strategy against International Terrorism and Radicalisation of 2012, and is aligned with the 2017 National Security Strategy. Its update for the period 2023–2027, scheduled for early 2024, began in November 2022 with the establishment of a multidisciplinary working group.

The ENCOT is, in turn, being developed through various sectoral strategic plans to combat terrorism-related activities, such as the **National Strategic Plan against Terrorist Financing** (PENCFIT) and the **Strategic Plan against Violent Radicalisation** (PENCRAV), both of which were approved on 6 October 2020 by the National Security Council. In 2024, work will begin on updating both Strategic Plans, which will then cover the period 2024–2028.

Since the implementation of the PENCFIT in October 2020 and the creation of Working Group III for the Plan's Monitoring and Follow-up (GRUSEFIT), 26 measures set out in the PENCFIT have been implemented.

These actions have taken the form of the adoption of inter-institutional cooperation agreements on information exchange, as well as legislative amendments and new initiatives, and training programmes aimed at both LEAs and magistrates, judges, Public Prosecutor's Office Special staff and legal advisers within the Audiencia Nacional

Furthermore, in the area of prevention, COPBLAC, at the proposal of the Standing Committee on Anti-Money Laundering and Countering the ***Financing*** of Terrorism (AML/CFT)**,** approved the ***'General Guidelines for the Strategy to Prevent the Use of the Financial System for Terrorist Financing'*** of 2018**.**

With regard to the PENCRAV, the Ministry of Home Affairs, through the Specialised Committee against Terrorism (hereinafter CECT), was designated as the body responsible for its development and implementation throughout the country, with CITCO also being tasked with coordinating these efforts.

The new PENCRAV aims to establish an effective framework for the prevention, understanding of the processes involved in, and response to violent extremism, in order to achieve a society that is more aware, informed, secure and resilient. It is designed as a flexible and up-to-date document, identifying various cross-cutting areas of action—referred to as *'spheres'*—and setting out their corresponding lines of action. Among the main areas worth mentioning are: training initiatives to combat radicalism and violent acts within the police sector; in the prison sector, the creation

of tools to provide information to judicial and prison authorities; and increased national and international cooperation through the creation of working groups and support for international projects.

7. MAIN VULNERABILITIES IN MONEY LAUNDERING AND TERRORIST FINANCING.

As set out in the 2020 NRA, the FATF adopts the following definition of vulnerability

"Vulnerability" *is any situation or circumstance that may be exploited or utilised by organisations or individuals seeking to carry out Money Laundering or* Terrorist *Financing activities*.

The aforementioned NRA identified a number of general areas of vulnerability which, across the board, could and can have an impact on Money Laundering activities in the various sectors.

A. Vulnerabilities arising from the population.
B. Vulnerabilities arising from geographical factors.
   - Transactions with high-risk territories or with their citizens/entities.
   - Transactions with countries where there is a greater presence of organisations or citizens linked to jihadist terrorism.
   - Transactions in the Gibraltar area.
C. Vulnerabilities arising from the nature of the organisation or the activity carried out.
D. Vulnerabilities arising from payment methods, the use of cash and the informal economy.
E. Vulnerabilities arising from technological innovations in financial transactions.
   - Vulnerabilities arising from the use of cyberspace.
   - Vulnerabilities arising from the use of cryptocurrencies or CA.

7.1. Vulnerabilities arising from the population .

The factors that characterise the vulnerabilities of migration flows continue to persist, primarily due to international capital movements which increase the risk of funds of illicit origin or intended for illicit purposes being channelled into the international financial system.

The digitisation of international remittances is now a reality, and has in turn been driven by the COVID-19 pandemic and the emergence of new non-financial intermediaries offering payment services.

Spain had a population of 48,085,361 at the end of 2022, of whom 6,089,620 were foreign nationals (12.7 per cent of the population). The largest community comes from Morocco, with 893,953 people (representing a 25.2 per cent increase in the population compared with 2019), followed by Romania (629,755), Colombia (453,911), Italy (301,791), the United Kingdom (284,037), Venezuela (278,159) and China (219,929)[17] .

Furthermore, irregular migration flows continued to be recorded in 2022, although the number of irregular migrants fell by 25.6 per cent this year compared with the previous year.

Data from the Banco de España show that remittances sent from Spain have increased by 10% compared with 2021 figures, with this increase concentrated in remittances to Paraguay, Colombia, the Dominican Republic and Morocco[18] .

[17] INE data.
[18] See Table 17.6a of the Banco de España's Statistical Bulletin.

Despite this digitalisation, it must be borne in mind that the use of cash by the migrant community is very high and poses a vulnerability to our system, as it makes it difficult to trace funds.

Another vulnerability stemming from immigration and the economic circumstances surrounding this section of the population is its susceptibility to being exploited by criminal organisations seeking to move funds derived from their criminal activities. In this regard, the role of the 'money mule' is particularly significant; this is a person who, in exchange for a commission, transfers funds on behalf of these criminal groups.

7.2. Vulnerabilities arising from geographical factors .

7.2.1 Conducting transactions with high-risk territories or with citizens/entities from those territories.

In line with the 2020 NRA, transactions carried out in Spain with high-risk territories or with citizens or entities from such jurisdictions are considered a vulnerability.

The first aspect of geographical vulnerabilities stems from transactions with jurisdictions that have strategic shortcomings in their Money Laundering (ML) and counter-terrorist financing (CTF) systems. For this reason, the FATF and the European Commission draw up and regularly update lists of high-risk countries, which Spanish institutions must always take into account when implementing their ML and CTF preventive measures.

In this regard, the lists of non-cooperative countries in tax matters, drawn up by Spain and the EU, must also be taken into account, as these jurisdictions may present a higher risk of Money Laundering due to their lack of transparency and their tax regimes.

Various criteria for identifying high-risk territories are set out in the Guidance on Geographical Risk in relation to Money Laundering/Terrorism, issued by COPBLAC[19] , which aims to provide guidance to obliged entities in this area.

In any case, it is the responsibility of each regulated entity – depending on the sector in which it operates, the type and volume of transactions it carries out, its professional experience and, above all, its own risk assessment – to determine whether there are other risks arising from doing business with certain countries or their nationals.

The **main risk criteria** to be taken into account are whether countries:

a) Do not have adequate systems in place to prevent Money Laundering and terrorist financing.
b) Are subject to sanctions, embargoes or similar measures adopted by the European Union, the United Nations or other international organisations.
c) Have significant levels of corruption or other criminal activities.
d) Provide funding or support for terrorist activities.
e) Have a significant offshore financial sector ('offshore' centres).
f) Are regarded as tax havens.

Consequently, the nationality or residence of the customer or their beneficial owner, the origin and destination of the funds, and the presence of any intermediaries, become risk factors to be taken into account; consequently, institutions must exercise extreme caution when analysing the risks of transactions in cases where customers or their funds have links to countries considered to be of particular risk in each activity and carry out transactions with those jurisdictions.

[19] http://www.tesoro.es/sites/default/files/guia_riesgo_geografico_en_materia_de_bc_ft.pdf.

The classification of a jurisdiction as high-risk is primarily determined by the FATF's so-called grey and black lists *(Jurisdictions under Increased Monitoring/High-Risk Jurisdictions subject to a Call for Action)* and the European Commission's lists of high-risk third countries *(High-risk third countries – Delegated Regulation (EU) 2016/167).*

According to information from SEPBLAC, reports of transactions involving high-risk jurisdictions were 9 per cent lower in 2022 compared with 2021.

7.2.2. Transactions with countries posing the highest risk of Terrorist Financing.

Due to its geographical location, Spain is one of the countries most vulnerable to Terrorist Financing and to recruitment and the recruitment of followers by terrorist organisations linked to radical Islamism.

Furthermore, attention must be paid to the potential exploitation of Spain's trade relations with the Maghreb countries and the migratory flows of citizens from this region for such purposes. Additionally, attention must be paid to the greater vulnerability of sectors that regularly operate with countries whose political systems might directly or indirectly support radical groups in their religious or ideological stances.

To combat these risks, it is essential to correctly identify the funds, as well as those involved in the process of receiving remittances in Spain, by ensuring that financial institutions have robust preventive systems in place.

7.2.3. Activities in the Gibraltar area.

According to the 2022 National Security Report, this is an area particularly vulnerable to being exploited by criminal groups for drug trafficking and smuggling, with a high exposure to the risk of Money Laundering and terrorist financing (ML/TF) and a high vulnerability to the commission of crimes and offences of this nature by land, sea or air.

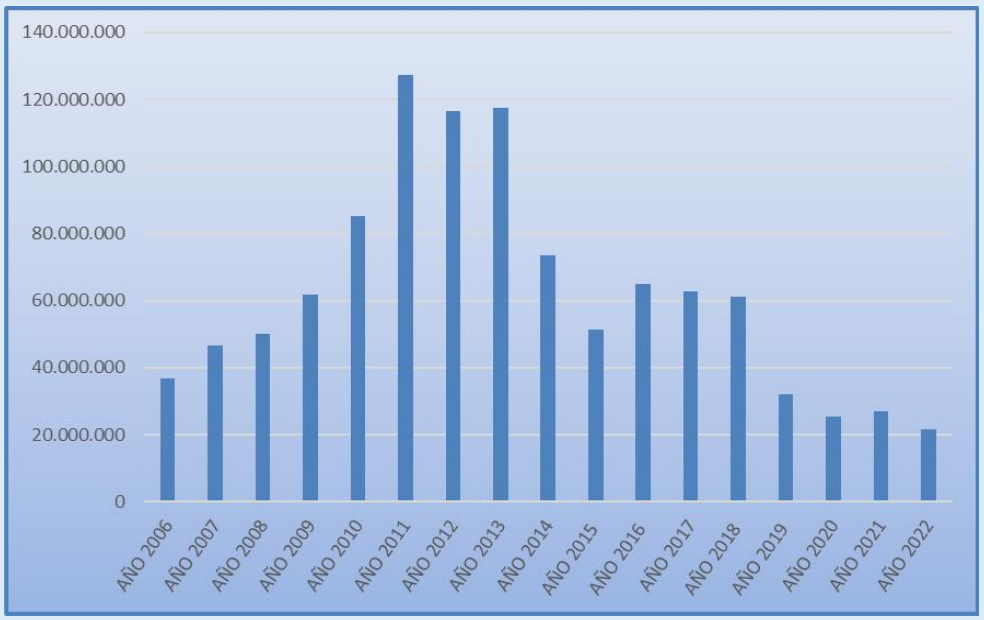
As mentioned in the section on threats, the Third Special Security Plan for the Campo de Gibraltar was geographically expanded to include three additional provinces (Almería, Seville and Granada) within its scope of action, with the aim of combating criminal groups involved in drug trafficking and smuggling.

In this regard, according to data from the Ministry of Home Affairs, the increase in detected drug trafficking offences—which statistics show has risen by 14.4 per cent since 2019—is attributable to the actions of the LEAs within the framework of specific operations such as the Special Security Plan for the Campo de Gibraltar. As already noted in the previous NRA for 2020, account must also be taken of the vulnerability posed by the borders of Ceuta, Melilla and Gibraltar to the smuggling of goods (tobacco, mobile phones, electronic equipment, etc.), which generates significant cash flows.

Data on declarations of cash movements at the border show that, of the three selected borders, Gibraltar stands out as the customs post with the highest number of declared cash outflows, accounting for 73 per cent of declarations. As regards declarations of cash inflows, Melilla ranks first with 67 per cent of declarations.

With regard to smuggling, it should be noted that despite the closure of the commercial customs posts in Ceuta and Melilla in 2019 and their reopening in January 2023, the data show that this criminal activity remains a recurring issue in our country, albeit with a lower incidence, particularly with regard to tobacco imports from Gibraltar, the incidence of which has been declining since 2014.

CUADRO 9. Entradas de tabaco desde Gibraltar (2006-2022)



Fuente: A.E.A.T.

With regard to drug trafficking, criminal operations by organised crime groups have been detected involving the use of cash, the acquisition of luxury goods or the purchase of property.

7.3. Vulnerabilities arising from the nature of the entity or activity carried out .

When analysing the vulnerabilities that may be exploited by criminal networks to carry out Money Laundering activities through the use of entities in different sectors, it is necessary to distinguish between endogenous and exogenous risks that may exist in each type of entity or activity.

Among the intrinsic or 'endogenous' risk factors arising from the entity itself or the activity it carries out are:

a) The possibility of setting up or acquiring entities or businesses for the purpose of concealing Money Laundering activities arising from unlawful activities or for the purpose of committing terrorist financing. In Spain, almost all obliged entities belong to sectors subject to licensing, registration and compliance with authorisation requirements, and are subject to a regime of prudential supervision and Money Laundering/terrorist financing prevention.
b) The possibility that Money Laundering/Terrorism Financing networks may exercise direct or indirect control over an entity's operations.
c) The possibility that employees or agents of certain types of entities may have links to criminal networks, which would enable the use of sophisticated and elaborate systems for handling illicit funds without the entity's knowledge and making such activities more difficult to detect.

Extrinsic or 'exogenous' risk factors are those that may allow an entity to be exploited by networks for Money Laundering/Terrorism Financing (ML/TF) purposes; in other words, it is not that the entity itself poses a risk, but rather

that an entity operating normally may possess a number of characteristics that render it vulnerable and susceptible to being used for ML/TF operations for various reasons, such as:

> A possible lack of commitment on the part of the entity to Money Laundering/CFT policies and measures. This may be due to a deliberate failure to implement preventive policies because of the cost of implementation, to negligent ignorance regarding the extent to which these measures have been developed within the entity, or to the priority given to the revenue generated by allowing greater laxity in the implementation of the required controls.
>
> An excessive volume of transactions with certain countries or the presence of a large number of customers of certain nationalities may be reasons for using a particular type of institution for Money Laundering/CFT operations. The absence of information or adequate procedures enabling the authorities to obtain precise knowledge of the beneficial owners of customers that are legal entities. A lack of a preventive culture amongst those institutions that become newly regulated entities

In addition, there may be a failure on the part of the competent authorities to communicate risk factors and to update relevant guidelines and regulations. These are risk scenarios that preventive policies must address, and which require greater vigilance and rigour on the part of national authorities through the regulatory and supervisory mechanisms at their disposal.

7.4. Vulnerabilities arising from payment methods, the use of cash and the informal economy[20] .

The COVID-19 pandemic led to a shift towards a more digital way of life, a development that also had an impact on the use of payment methods. At the same time, the digitalisation of livelihoods and the economy can help to reverse the trend of depopulation in rural areas.

According to the Banco de España's *2022 Study on Cash Usage Habits*, cash is the most frequently used payment method, followed by cards and mobile devices (phones and smartwatches), with three in five Spaniards using cash on a daily basis, particularly those with basic education and those aged over 45.

In this study, cash once again ranks first as the retail payment method used in 2022, with daily use by 64 per cent of the population, whilst in 2021 it accounted for 35.9 per cent[21] ; in 2022, bank cards were the payment method used by 32 per cent of the population.

As regards the introduction of non-traditional payment methods and looking at their occasional (non-daily) use, mobile devices rank as the third most common payment method, behind cash and bank cards. Meanwhile, the new payment service provider (*Bizum*) is used by 44 per cent of the population, although daily use of it as a payment method has fallen to 1 per cent.

With regard to obtaining cash, 79 per cent withdraw it from ATMs, mainly in amounts between 20 and 50 euros. However, 6 per cent of the population obtains cash from non-bank sources – that is, from family, friends or work – which highlights the vulnerability of this payment method to Money Laundering and terrorist financing.

This risk is particularly prevalent in areas without a permanent bank branch, where 66.4 per cent of the population living in rural areas have an ATM more than 1 km away. In such cases, the informal economy and tax evasion become the main vulnerabilities in the fight against Money Laundering.

[20] Source: *Study on cash usage habits 2022*, Banco de España.
[21] 2021 Annual Cash Survey, Banco de España.

However, new technologies have led to the introduction of digital payments, driven by changes under PSD2 and the emergence of new operators offering new payment instruments, methods and services.

Taking into account the use of new, more digital payment methods, a number of risks have been identified:

- An increase in fraudulent transactions linked to phishing scams, where debit or credit card details are obtained and access to e-wallets is gained.
- The use of new methods that facilitate the concealment of, and lack of transparency regarding, the origin of funds.
- Identity theft or the provision of identity in exchange for compensation (money mules) to set up payment instruments that allow funds of illicit origin to be introduced into the system.
- The global nature of payment methods, which operate without border barriers, and the lack of tools to effectively trace the flow of funds.

The Spanish regulatory framework has been adapted to the new reporting requirements set out in European legislation regarding the declaration of payment instruments, through the adoption of the administrative measure on Payment Instruments by Order ETD/1217/2022 of 29 November, which sets out the forms, criteria and reporting procedures applicable to those who, acting on their own behalf or on behalf of a third party, carry out the payment transactions provided for in Article 34 of Law 10/2010 of 28 April.

7.5. Vulnerabilities arising from technological innovations in financial transactions[22] .

7.5.1. Vulnerabilities arising from the use of cyberspace.

The digital transformation of society, public administrations and the financial system has, on the one hand, streamlined and facilitated the lives of citizens and businesses in certain respects; however, on the other hand, reliance on information technology has led to an increase in Money Laundering/Terrorism Financing risks, as well as vulnerabilities to potential cyber-attacks.

These vulnerabilities have increased due to the possibility of suffering such attacks, given the technical sophistication of these attacks and the implementation of effective security measures that allow their origin to be concealed.

The digitalisation of public administrations brings great opportunities, but at the same time they face vulnerabilities arising from the use of technology. According to the 2022 National Security Report, the Ministry of Defence, for example, has suffered 2,035 *cyber incidents*. This reflects the growing efforts by cybercriminals to attack the databases of public authorities and public service organisations, with the aim of obtaining personal data for use for spurious purposes, often within the criminal sphere.

Among the types of cyberattacks to which Spain is currently exposed, computer fraud associated with scams stands out; the most common forms of cybercrime in Spain are technical support and investment scams, *Business Email Compromise* (BEC), as well as mass phishing campaigns and, increasingly, *smishing*.

With regard to Terrorist Financing, cyberspace has become an easily accessible tool for terrorist organisations, enabling them to disseminate their message instantly and gain access to new forms of financing that facilitate the concealment of funds and the loss of traceability through the use of appropriate techniques.

[22] Source: National Security Report 2022.

Spanish financial institutions, aware of this problem, allocate a significant proportion of their human and financial resources to the cybersecurity of their technological systems. According to recent studies, average expenditure in this area stands at 10 per cent of the annual budget.

7.4.2 Vulnerabilities arising from the use of virtual currencies and assets.

The very nature of virtual currencies highlights the vulnerability to which the financial system may be exposed when they are used, due to their ability to: i) carry out cross-border transactions rapidly outside the regulated financial system, ii) conceal the origin and destination of funds, and iii) make it difficult for regulated entities to detect suspicious transactions.

Furthermore, the specific design of the CA may prevent the application of traditional traceability techniques. There is evidence of increased use of these private CAs as facilitators of cybercrime, which is particularly notable in cases of *ransomware*.

Similarly, the inherent characteristics associated with their underlying technology (the blockchain) facilitate a degree of anonymity in certain types of transactions or certain types of CAs, which may hinder the detection of criminal activities by the authorities.

However, the mere presence of these characteristics in an activity does not automatically imply an unlawful operation. For example, the use of *cold wallets* – whether *hardware-based* or paper-based – can be a legitimate means of protecting oneself against theft.

Similarly, the use of applications that allow access to the so-called *deep web* – making it almost impossible to detect such operations in advance – enables criminals and members of organised crime to utilise these methods to conceal criminal activities, and means that a large proportion of payments on these websites are made using CA.

Finally, one of the cybersecurity vulnerabilities that can affect this sector is direct attacks on CASP. In Spain, the Guardia Civil, as part of 'Operation 3COIN', dismantled a cybercriminal group in the summer of 2020 that had launched a direct attack on a cryptocurrency custodian company, resulting in losses of 6 million euros.[23]

Currently, three of the ten most active CASP in Spain are registered in the country. These CASP account for 60.2 per cent of the activity of these *exchanges*[24] .

8. SECTOR-SPECIFIC RISKS.

The purpose of this NRA is to analyse those sectors that have undergone substantial regulatory changes, new trends in their operations, or factors or characteristics that necessitate an update from the perspective of the risks of engaging in Money Laundering activities since the previous version of the NRA, approved in 2020. For sectors already covered in the 2020 NRA, however, the update carried out in this analysis does not entail a change in the risk assessment previously assigned, with the exception of payment transactions carried out by payment institutions, where the risk has been upgraded from moderate to significant. In addition, the analysis of CAs and CASP has been completed; the 2020 analysis was much more general in nature and focused on a broad analysis of services involving virtual currencies and assets. Taking into account the variables mentioned in the following sub-sections, the following sectors will be analysed:

[23] https://www.guardiacivil.es/es/prensa/noticias/8134.html?versionImprimible=true
[24] Among the 50 most active CASP's analysed by Chainalysis.

Risks in the financial sectors:

a) Securities investment services, managers of collective investment schemes and securitisation managers.
b) Money remittance by payment institutions.
c) Other services provided by payment institutions.
d) Electronic money transactions.
e) Crypto-assets and crypto-asset service providers.

Risks in non-financial sectors:

a) Activities carried out by notaries.
b) Activities carried out by land, commercial and chattel registrars.

8.1. Risks in the financial sector.

a) Investment services, collective investment schemes and management companies.

Activity, context and regulatory framework.

The update to this sector has been prompted by the amendment to Law 6/2023 of 17 March on Securities Markets and Investment Services in Spain, regarding the possibility of representing securities using distributed ledger technology (DLT), in addition to the systems of representation already provided for through certificates or book entries.

Law 6/2023 of 17 March covers, amongst other matters, the issue and offering of financial instruments; the authorisation regime, operating conditions and prudential regime for investment services firms; the provision of investment services and activities in Spain by firms from third countries; and the supervisory, inspection and sanctioning regime administered by the National Securities Market Commission. The scope of the Law covers various financial instruments, including transferable securities, money market instruments, shares and units in collective investment undertakings, in venture capital firms and in closed-end collective investment undertakings, and various derivative instruments such as options, futures and contracts for difference.

Furthermore, the sector is also regulated by Law 35/2003 of 4 November on Collective Investment Undertakings (CIUs or open-ended undertakings) and by Law 22/2014 of 12 November, which regulates venture capital firms, other closed-end collective investment undertakings and management companies of closed-end collective investment undertakings.

These entities are subject to prior administrative authorisation by the CNMV. The authorisation process requires compliance with the obligations set out in the regulations and the issuance of a preliminary report by SEPBLAC regarding the suitability of the preventive bodies and procedures that the entity being set up intends to implement should the requested authorisation be granted. The CNMV is the competent authority for the prudential supervision of securities markets and their activities, whilst supervision relating to the prevention of Money

Laundering and terrorist financing is carried out by SEPBLAC and, in the event of a Memorandum of Understanding, by the CNMV. This Memorandum of Understanding was signed on 7 July 2023.

With regard to the registration of securities using DTL technology, it should be noted that, in practice, no initiative has yet been launched regarding this possibility within the securities market. This initiative entails new risks, primarily in the business model, due to the emergence of new *players* and possible changes in the roles of the entities involved, as well as opportunities arising from the creation of a single database that generates benefits in terms of efficiency, operational risks and costs.

- **Investment services.** In Spain, alongside credit institutions, investment services firms (ESI) may provide investment services:

- **Securities firms and securities agencies**. The difference between the two is that securities agencies cannot carry out investment activities on their own account; their activity therefore consists of providing investment services to third parties, whilst securities firms may also act on their own account, as well as being able to provide underwriting services and the ancillary service of granting credit for securities trading.
According to data from the CNMV Register, as at 31 December 2022 there were a total of 35 securities firms and 60 domestic securities agencies. In addition, there are some 900 EU investment firms (ESIs) that can use the EU passport to operate in Spain under the freedom to provide services, and a further 51 EU entities with branches in Spain. The number of European investment firms authorised to operate in Spain under the freedom to provide services has fallen significantly following Brexit.

- FAFs offer their clients, as their sole reserved activity, financial investment advisory services. They may not act as custodians for clients' securities or cash. They must hold the required authorisation and be registered with the CNMV. As of December 2022, there were 143 registered FAFs, which collectively had 11,000 clients – of whom approximately 10,000 were retail clients – an advised portfolio of 19,000 million euros and 49 million euros in advisory revenue. Most FAFs serve retail clients, whilst 32 of them serve professional clients exclusively. As can be seen, their significance is, for the time being, limited.

In addition, the regulations provide for another specific type of ESI: portfolio management companies (SGCs), which may only provide the investment service of discretionary portfolio management; however, as at 31 December 2022, none were listed in the register. This is explained by the preference for obtaining authorisation as securities firms or agencies, which allows them a broader scope of activities.

- **Collective investment**. **Collective Investment Undertakings (**CIUs) are financial institutions whose purpose is to invest in assets held in common on behalf of a group and to distribute returns to investors in accordance with the collective results. CIIs may be set up as **investment funds** or as **investment companies**. In both cases, a financial institution is required to act as custodian of the vehicle's portfolio; however, investment funds must always have a management company (SGIIC), as they lack legal personality, whilst investment companies may manage their own assets or use a management company, although the vast majority are also managed and administered by SGIICs. Almost all Spanish SGIICs (investment funds and investment companies) are members of INVERCO, the Association of Collective Investment Institutions and Pension Funds.

-Investment funds can fall into different categories:

- **Financial asset investment funds**. These are owned by a number of investors who subscribe to units in the fund. They are the main collective investment vehicle. According to data from the CNMV, in December 2022 they had assets under management of 315,798 million euros.
- **Property investment funds**. These invest in property assets with the aim of generating income from letting. They are governed by the provisions applicable to financial funds. They must have a minimum of 9 million euros

paid in. As of December 2022, there were only two registered funds, both of which were in the process of being wound up.

- **Open-ended investment funds** (*"Hedge Funds"*). These are complex products in which the manager adopts various strategies to maximise returns for fund unit-holders. They are generally aimed at qualified investors (high-net-worth individuals, institutional investors, professional entities). Their main feature is that they can invest without the restrictions imposed on other funds (all types of assets, diversification of investments and the use of leverage). Consequently, they offer the potential for higher returns, but also a greater risk of losing the investment. According to data from the CNMV, there were 54 hedge funds registered in Spain as of December 2022.

- **Open-ended investment companies** (SICAVs), as well as property investment companies (SIIs) and hedge funds (SILs). SICAVs, which are the most widespread of the three, are public limited companies whose corporate purpose is to invest in financial assets, and whose shareholders are the investors themselves. They require a minimum of one hundred shareholders and €2.4 million. They are subject to a 1 per cent tax rate if they meet certain requirements. In December 2022, there were 21,091 SICAVs in Spain with assets totalling 15,785 million euros. Their number has been declining in recent years. The number and assets of SIIs and SILs are significantly lower than those of SICAVs.

- **Collective investment scheme management companies** (SGIICs) are public limited companies that administer and manage the aforementioned investment funds and companies, acting in the interests of unit-holders and shareholders. They may also act as administrators and managers of closed-end vehicles. SGIICs are subject to various requirements and must publish certain individualised information for each investment fund (documents containing information for investors; prospectus; annual report including the management account and annual accounts; and quarterly/half-yearly reports on assets under management, the number of units or shares in issue, securities held in the portfolio, etc.).

At the end of 2022, there were 123 collective investment scheme management companies registered with the CNMV, managing assets of around 350,000 million euros in collective investment schemes, mainly in financial investment funds. The sector is highly concentrated, as the three largest SGIICs have a combined market share of approximately 40 per cent of total assets.

- **Closed-end collective investment undertakings: Venture capital funds and companies, and other closed-end vehicles**. These are collective investment undertakings which, having no commercial or industrial objective, raise capital from a number of investors through marketing activities, in order to invest it in all types of financial or non-financial assets, in accordance with a defined investment policy. In the case of the sub-type comprising venture capital funds and companies, their purpose is to invest temporarily in unlisted companies that are neither financial nor property firms, with a view to increasing their value and generating a return on the investment made. These closed-end vehicles resemble UCITS in their nature as collective investment schemes, but differ in terms of greater flexibility regarding their potential investments, lower liquidity and the fact that they are primarily aimed at professional investors, although they are increasingly being marketed to retail investors. They invest primarily in companies in the technology and services sectors, or in renewable energy, mainly in start-ups or restructured companies, with high growth potential and higher risk. They are managed by closed-end fund management companies (SGEIC) or by SGIICs.

Management companies (SGEIC, formerly known as SGECR) are dedicated to the administration and management of closed-end funds and the assets of closed-end companies. According to the CNMV register, at the end of 2022 there were 482 fund vehicles organised as companies (of which 319 were venture capital funds (FCR), 56 were closed-end investment funds (FICC), and the remainder were other fund-structured vehicles), and 373 corporate-structured vehicles (of which 319 were private equity companies (SCR) and the remainder were other corporate-

structured vehicles). In 2022, private equity and venture capital investment totalled 9,238 million euros across a total of 958 investments[25] . International operators accounted for 80.2 per cent of total investment, with a very significant presence in large transactions.

Threats.

Operations in this sector require a certain level of investment expertise; consequently, in terms of Terrorist Financing, the threats are low and the likelihood of terrorist organisations using this channel to channelling their funds is minimal, and decreases as a higher investor profile is required.

The same line of reasoning can be applied in the case of Money Laundering. However, the existence of factors such as over-the-counter trading, fraud that may be carried out through so-called 'financial shacks', or the misappropriation of funds resulting from corruption, increases the risk of investment services being used for illicit purposes. Factors that may influence money laundering include the service being established from the outset as criminal in nature, as in the case of investment fraud, or the use of high-net-worth individuals to channel funds obtained illegally.

Vulnerabilities and sector-specific risk.

This sector is characterised by the diversity of the players and products within it, which can give rise to different types and levels of risk. Furthermore, account must be taken of the interaction between the sub-sectors and, above all, the direct relationship with other parts of the financial sector, particularly the banking system, which plays a very significant role both through the direct provision of investment services and because a large proportion of the aforementioned entities providing investment services, collective investment schemes and other services belong to banking groups.

Thus, in the area of investment services, by the end of 2021 banks reported almost 12 million clients, assets under management of 116,000 million euros, securities held in custody amounting to 3.5 trillion euros, and revenue from investment services amounting to 6,000 million euros, compared with far more modest figures for ESIs: 300,000 clients (40 times fewer), €9,000 million in assets under management (13 times less), €72,000 million in securities held in custody (50 times less), and €900 million in revenue (7 times less). Meanwhile, in the field of collective investment, the assets under management attributable to banking groups account for more than 80 per cent of the total under management. In short, supervisors, investigators and financial intelligence analysts highlight Money Laundering/Terrorism Financing (ML/TF) risks associated with these activities, primarily in relation to the following **vulnerability** factors:

- The use of corporate structures that may make it difficult to identify the beneficial owner of the securities.
- The use of complex channels that may make it difficult to trace the origin and flow of the funds invested and that facilitate investor anonymity.
- The characteristics and origin of investors and their intermediaries, particularly where they have links to high-risk jurisdictions (*offshore centres*, tax havens, designated territories or those deemed non-cooperative in tax matters or in the fight against Money Laundering), as well as clients who are public officials and cases where clients act through nominee holders.
- The existence of unlicensed service providers whose activities are facilitated by the use of new technologies and the increasing use of online channels to provide such services.
- A lack of awareness of the risks associated with the use of distributed ledger technology (DLT) for the registration of securities.

[25] Data from SPAINCAP.

Furthermore, the use of *blockchain* technology will require the issuer to appoint one or more entities responsible for the registration and recording of securities in the system; amongst other functions, these entities will manage the identification of holders of rights derived from negotiable securities, as well as the various corporate events, registrations or encumbrances affecting the issue. Regardless of this, these designated entities must be authorised to provide securities custody services, an activity reserved by Law for registered investment service providers, primarily banks and investment firms. This helps to limit the risks associated with money laundering.

As noted by the EU's SNRA, although the risk of terrorist financing (TF) is low, there is a growing risk of Money Laundering (ML) through capital markets, particularly via providers of such services or through the use of complex, cross-border schemes that facilitate the use of these products to conceal the origin of funds and/or their owners.

However, given their interaction with the banking sector when contracting investment services, the risks of these products being used for such purposes are reduced, bearing in mind that the Spanish banking sector has a solid and robust preventive system in place. Nevertheless, when financial institutions or intermediaries based in high-risk jurisdictions—whether offshore or not—are involved, and there is no certainty that European standards on AML/CFT are being met, the risks increase and the Spanish financial sector's vulnerability to AML/CFT risks is heightened.

In any case, when used for Money Laundering purposes, factors such as the financial viability of the product or the need to ascertain the quality of the investment act as a deterrent to the use of these instruments. However, when criminal networks can rely on more complex financial planning and use professional facilitators for this type of service, there may be greater incentive to use them for Money Laundering purposes.

It is worth noting that the sector is highly aware of the risks of Money Laundering and terrorist financing. Beyond regulation and legal due diligence obligations, investment service providers and management companies are implementing increasingly comprehensive and complex internal control systems for the prevention of Money Laundering and terrorist financing, continuously adapting to the needs of the financial system. Custodian institutions, which are essential to these services, also have preventive duties.

Conclusion.

Money Laundering risks. The inherent risk of investment services being used for Money Laundering activities is **high**, owing to the very purpose of generating financial returns on invested funds and the existence of various vulnerabilities arising from the types of investment products and investment channels, which can help to conceal the origin of funds and the identity of the beneficial owner. However, the regulation and supervision of these services, the awareness among sector entities regarding the implementation of ML/TF prevention measures, and the indicated mitigation measures aimed at controlling the activities of such entities serve to reduce the residual Money Laundering risk, which should be classified as **moderate/significant**, depending on the product and the profile of its clients.

TF Risks. Unlike Money Laundering risks, the very nature of these types of services—which are linked to the financial returns of products—makes them more difficult to use for TF purposes and less attractive and exposed to such use; consequently, the residual risk of securities investment services, financial services provided by collective investment scheme managers, and securitisation fund management companies being used for TF activities is considered to be **low.**

b) Money transfers by payment institutions.

Activity, context and regulatory framework.

The need to update this sector has arisen due to the ongoing threats surrounding the money transfer business and the evidence gathered through supervisory activities.

Money transfers to or from abroad by payment institutions, commonly referred to as remittances and known internationally by their English acronym MVTS ([26]), are considered by the FATF and the EU's SNRA report to be particularly vulnerable to Money Laundering/Terrorism Financing.

Regulation 847/2015 on fund transfers, has been amended by Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying fund transfers and certain credit transfers and amending Directive (EU) 2015/849. This Regulation defines fund transfers as *"any transaction carried out at least partly by electronic means on behalf of a payer through a payment service provider, with the aim of making funds available to a payee through a payment service provider, regardless of whether the payer and the payee are the same person and whether the payer's and the payee's payment service providers are the same, including: a) credit transfers, as defined in Article 4(24) of Directive (EU) 2015/2366; (b) direct debits, as defined in Article 4(23) of Directive (EU) 2015/2366; (c) money remittances, as defined in Article 4(22) of Directive (EU) 2015/2366, whether domestic or cross-border; d) transfers carried out using a payment card, an electronic money instrument, a mobile phone or other digital or IT device, whether prepaid or postpaid, with similar characteristics".*

Royal Law 19/2018 of 23 November on payment services and other urgent measures in the financial sector, which transposes the European Payments Directive, defines *a "money remittance service"* as *"a payment service that enables funds to be received from a payer without any payment account being opened in the name of the payer or the payee, for the sole purpose of transferring an equivalent amount to a payee or to another payment service provider acting on behalf of the payee, or of receiving funds on behalf of the payee and making them available to the payee"*

In the EU's SNRA, this activity is analysed as *"Money transfers or remittances"*, a payment service that utilises both cash and electronic transfers.

Traditionally, this service has been known as remittances sent by migrants to their countries of origin. Although the usual method for these money transfers is the use of cash – whether due to a lack of access to banking services amongst this population, the receipt of funds from the informal economy, or because it is a traditional way of sending money – transfers or the use of cards via online money transfer platforms developed by these traditional *remittance companies* are becoming increasingly important.

Most of the customers of such organisations are migrants from Latin American, North African and Asian countries, and it is also common for some businesses acting as agents for payment service providers ( ) to be run by people of

[26] Money and Value Transfer Services.

these nationalities, whilst simultaneously carrying out other non-financial economic activities in the same premises, such as the so-called *'locutorios'.*

The service of sending money without the need to open a payment account is reserved for payment institutions. These institutions are regulated by Royal Decree-Law 19/2018 of 23 November on payment services and other urgent measures in the financial sector.

Payment institutions are subject to authorisation by the Banco de España, following a report from SEPBLAC on the suitability of their governance bodies and anti-money laundering procedures. Once authorisation has been obtained, and following registration in the Commercial Register, the institution will be entered in the Special Register of Payment Institutions, in which its agents and branches must also be listed. Prudential supervision of compliance with and maintenance of the conditions of authorisation is the responsibility of the Banco de España, whilst supervision of anti-money laundering and counter-terrorist financing (AML/CTF) measures falls to SEPBLAC, as well as to the Banco de España in the event of an agreement, signed on 18 March 2021.

The volume of business carried out by these institutions in Spain amounts to 18,026,[27] million euros (11,570 million money orders issued and 6,456 million money orders received), with 89 per cent of the sector's total activity concentrated in 10 institutions.

The average value of remittances is estimated at 260 euros, and the top 10 destination countries for remittances sent are (in millions of euros): Colombia (1,112), Morocco (991), Ecuador (668), the Dominican Republic (484), Pakistan (432), Honduras (404), Bolivia (396), Senegal (383), Paraguay (375) and Peru (354)[28] .

As at 31 December 2022, the sector comprised 52 payment institutions established in Spain, of which 25 are authorised to provide money transfer services and 21 provide this service exclusively. The sector is highly concentrated, with the ten leading entities accounting for nearly 80 per cent of the total volume. Almost half of these entities (19) belong to the Spanish Association of Payment Institutions (AENPA).

In addition to these entities, there are 10 payment institutions exempt under Article 14 of Royal Decree-Law 19/2018 of 23 November, which carry out money remittance activities. These entities are obliged entities as set out in Article 2.1(h). Article 2(3) provides for the possibility of excluding these entities, either wholly or in part, provided they present a low risk of Money Laundering and terrorist financing.

According to data from the Banco de España, these entities have carried out 73,352 money transfer transactions totalling almost 27 million euros. In comparison with money transfer activity, it can be seen that the operations of these entities falling under the regulation of Article 14 of Royal Decree-Law 19/2018 of 23 November are not significant.

Threats.

Remittances sent to high-risk jurisdictions, particularly those identified by the FATF in relation to Terrorist Financing, pose significant ML/TF risks. The possibility of splitting remittances, the use of cash or prepaid cards to send funds, and the fact that little financial expertise is required to carry out these transactions make this financial service an easily accessible channel for Terrorist Financing.

Criminal organisations use this channel to channel their funds and make them harder to trace through such transfers, as well as to carry out the activity that constitutes the source of the crime.

[27] Estimate as at 31 December 2022, produced by SEPBLAC based on its own data and data from the Banco de España. SEPBLAC's data accounts for 50% of the activity.
[28] Data obtained from the activity of these entities reporting to SEPBLAC as at December 2022.

Fraud is particularly prevalent in the use of such services, both in well-known fraud schemes such as *'Nigerian letters'* and in the movement of funds obtained through *phishing* scams or tax fraud. Furthermore, drug trafficking, human trafficking and the smuggling of goods are crimes that make extensive use of these money transfer services.

Potential money laundering operations involve not only splitting transfers among multiple senders to destination countries to avoid detection (activities known as *'smurfing'*), but also the takeover of these agencies by networks (outside the financial institution), which enables money transfers to be made by impersonating senders or by falsifying their identities through agents linked to the Money Laundering networks themselves.

In Money Laundering offences associated with money transfer operations, the role of *the 'mule'* is particularly significant; this is the individual who, in exchange for payment, acts as the main agent in the transfer of funds. In this regard, although cash remains the primary instrument used, it is considered necessary to mention prepaid cards, which do not require the opening of a payment account. Loading cash onto these cards and subsequently using them to send funds via money transfer platforms constitutes an additional method for moving cash flows originating from the criminal activities outlined above.

Vulnerabilities and sectoral risk.

The **inherent risk** in the payment institutions sector is very high[29] for various reasons, relating to both endogenous and exogenous factors.

The total number of foreign nationals residing in Spain at the end of 2022 stood at 6,089,620 people, representing 12.7 per cent of the population. The use of cash amongst this section of the population is high, mainly due to the informal economy associated with their economic activities and remittance transfers to their countries of origin.

Payment institutions and their branches and agencies present a higher risk than other regulated entities due to their capacity to channel funds, which makes them an attractive system for transferring illicit funds. This is due, on the one hand, to the fragmentation of their operations, as a large number of customers carry out many small-value transactions, and, on the other hand, to the existence of a significant number of small-scale establishments that handle money transfers on an agency basis (each payment institution may have thousands of agents). All of this makes it difficult for the authorities and the payment institutions themselves to exercise adequate control over these establishments, a situation which, in previous years, has encouraged criminal networks to use agents and small establishments for Money Laundering activities.

In this regard, the agent plays a key role in the prevention of money laundering due to the vulnerability this role represents in the face of Money Laundering/Terrorism Financing risks, as the high turnover of agents between different payment institutions and their direct relationship with the customer allow them to foster a sense of loyalty that is more focused on the service provided to the customer than on regulatory compliance with the managing entity.

These factors make it difficult for the authorities to control and supervise these establishments, making them an attractive system for criminal and terrorist organisations to transfer illicit funds.

Residual risk. The implementation in recent years of risk-based Money Laundering/CFT preventive measures in the money transfer sector has led to increased monitoring and supervision of these transactions and the adoption of specific preventive measures by payment institutions, which have resulted in a significant mitigation of risks. These measures include, in particular:

- The establishment of stricter customer due diligence obligations. Specifically, Spanish regulations require the identification and verification of the identity of the customer or any person carrying out an occasional

[29] In line with the findings of the EBA Report on ML/TF risks associated with Payment Institutions, published in June 2023.

money transfer transaction, regardless of the amount involved (unlike the requirement under the EU Directive – a threshold of 1,000 euros).

- The adoption of specific obligations regarding internal control policies for the prevention of Money Laundering and terrorist financing (ML/TF) within the sector.
- Requirement for a more rigorous system of systematic reporting via the Mandatory Monthly Declaration submitted by these entities, which requires detailed information on their activities in accordance with various classification criteria.
- Creation of a register of high-risk entities by the sector itself, through its association, AENPA.
- Stepping up supervisory actions and enforcement measures.
- Measures aimed at raising awareness amongst entities regarding the prevention of Money Laundering and terrorist financing.
- Existence of a Catalogue of Money Laundering/Terrorism Financing (ML/TF) Risk Transactions in the money remittance sector[30] .

For their part, payment institutions represent the second-largest group of obliged entities in terms of the number of suspicious transaction reports; specifically, the annual figures for reports submitted by institutions in this sector have averaged around 1,000 since 2017.

The result has been a substantial improvement in the implementation of preventive measures, with a strengthening and increase in controls and prevention policies; consequently, the risk associated with money transfers by payment institutions has fallen from high to significant.

Under no circumstances should the risk posed by payment institutions in relation to their customers' activities be linked to the potential risk posed by payment institutions as customers of other regulated entities. In this case, the improvement in the quality and quantity of the internal measures, policies and procedures adopted in recent years by payment institutions, together with the measures implemented by financial institutions, and the growing collaboration between these two types of institutions, mean that the overall residual risk has been significantly reduced and is set to continue falling.

Conclusion.

Money Transfer Activities Carried Out by Payment Institutions Carry Very **High** Inherent Risks of Being Used for Money Laundering and Terrorist Financing Purposes. However, These Risks Have Been Mitigated Through Various Actions and Measures, Which Have Yielded Very Positive Results in Terms of the Overall Reduction of Risks.

These measures, specifically targeted at money transfer operations, address various areas of action: strengthening the prevention framework by payment institutions; inspection activities carried out by supervisory authorities (90 between 2018 and 2022); reporting obligations; engagement with the sector by the authorities and the joint compilation of lists of high-risk transactions; coordination between entities in the sector and the monitoring of risk agents, amongst other actions.

All these mitigation measures implemented in recent years within the payment institutions sector have led to a substantial improvement in the sector's risk profile, which has shifted from high to **significant** for **Money Laundering** and **FT**.

[30] http://www.tesoro.es/sites/default/files/cor_entidades_de_pago.pdf.

c) Other services provided by payment institutions.

Activity, context and regulatory framework.

The update to this sector has been prompted by the increase in the number of payment transactions processed. In turn, access to the National Electronic Clearing System (hereinafter, SNCE) and the reporting of payment accounts by this sector to the FTF have facilitated the review of the sectoral risk profile set out below.

PSD2, transposed into Spanish law by Royal Decree-Law 19/2018 of 23 November, introduced the provision of payment services in addition to money transfers (analysed in the previous section): deposits into and withdrawals from payment accounts; transfers, direct debits and card payments (debit or credit); the issuance of payment instruments or the acquisition of payment transactions; payment initiation services or account information services. Payment institutions may not offer deposits or repayable funds, nor issue electronic money, amongst other restrictions on their activities.

As indicated in the previous chapter, as at 31 December 2022, the payment institution sector comprises 52 payment institutions established in Spain and registered with the Banco de España; in addition, 258 payment institutions without a physical presence in Spain, authorised in other European countries, are permitted to operate.

According to data from the Banco de España, 27 institutions offer services other than money transfers, although this figure includes four institutions authorised to carry out money transfers and other services.

PSD2 and its transposition into Spanish legislation laid the foundations for promoting innovation and the adoption of new technologies in banking services. In December 2021, the Regulation governing the SNCE in Spain was amended, allowing payment institutions and electronic money institutions to access the system.

In Spain, although payments are predominantly made by credit institutions or with their involvement, payment accounts linked to payment institutions or electronic money institutions are becoming increasingly common, promoting greater financial inclusion amongst the population. The Payment Services Directive (PSD2) and its transposition now regulate other services provided by payment institutions that are not subject to a specific framework. Specifically:

- Payment **initiation** services. These services enable a payment order to be initiated, at the user's request, in respect of a payment account held with another payment service provider. Consequently, a customer authorises the provider of these services to access their payment accounts in order to pay for their purchases or other services directly to the supplier, without the need to use a payment card or for the financial institution to act as an intermediary in the transaction.
- **Account aggregation** services**.** These services involve consolidating information on balances and transactions from various payment accounts that a single customer may hold with different financial institutions.

The nature of these services means that payment institutions which act exclusively as payment 'initiators' or account information 'aggregators' need only have the customer's consent and the information necessary to carry out their activities, without needing to act as administrators of the payment accounts, as they do not manage their customers' funds.

Threats.

Police investigations show that the use of this type of payment service—involving the creation of a payment account for the purpose of carrying out international transactions and executing payment operations to obtain the goods

or services necessary to conduct their operations and finance their activities—is a service utilised by terrorist organisations.

The transactional nature of these payment services poses threats to the Spanish preventive system, particularly when there is interaction with jurisdictions where the economy has limited access to banking services or which are considered to be at high risk of Terrorist Financing.

As regards Money Laundering, the threats are similar to those mentioned for money transfer services; this type of operation is facilitated by the digitalisation of the economy and access to these services online, together with the emergence of intermediaries acting as service providers whose payment infrastructure relies on an authorised payment institution.

As noted in the previous section, payment institutions are subject to authorisation, supervision and registration by the Banco de España.

Vulnerabilities and sector-specific risks.

Payment institutions may carry out immediate payment transactions involving the opening of payment accounts. This activity gives rise to risks, primarily regarding the difficulty of identifying the beneficial owner of such an account, which entails **high inherent risks**.

The emergence of new operators offering payment intermediation services between customers and institutions may lead to the widespread opening of payment accounts in the name of the intermediary, where all transactions by individuals operating through these intermediaries are recorded. This makes it difficult to identify the beneficial owner of the transaction, creating Money Laundering/CFT risks for the institution acting as the obliged entity.

In short, new technologies have created new markets in which operators offer new instruments based on electronic transactions carried out by the customer, which can be used or initiated from any terminal and anywhere in the world. At the same time, a vast range of services has been developed that go beyond payment activities.

As regards payment initiators and account information aggregators, it should be emphasised that they must obtain the customer's consent to provide their services and that they act merely as intermediaries between the payee and the customer, without needing to act as payment account administrators. For this reason, the payment initiation and account aggregation activities carried out by payment institutions present significantly **lower inherent risks**, as they do not, under any circumstances, manage customers' funds.

Furthermore, as there is no contractual relationship between these service providers and the account manager, the regulations on payment services require, in order to ensure the integrity of funds and the confidentiality of information: 1) that open, common and secure standards be used in communications between both parties, and 2) that all parties adopt security measures in their dealings.

In any event, in accordance with the requirements of EU regulations, these entities are regarded as obliged entities in the field of Money Laundering/CFT, and must therefore apply the same preventive controls to payment transactions and payment initiation operations, which further reduces these risks.

Finally, with regard to payment institutions that issue credit and debit cards, a contractual relationship is required with retail customers and entities that make purchases using their cards and authorise the payment institutions to set up a direct debit with the credit institution where those customers hold a bank account; that credit institution is, in turn, an obliged entity. For this reason, the activities carried out by these payment institutions that issue credit and debit cards present lower inherent risks, although they must also establish appropriate control mechanisms to prevent their misuse.

Conclusion.

On the one hand, the ability to execute payment orders and access the SNCE, which is made possible by the creation of payment accounts, poses a risk of these accounts being used for Money Laundering activities. Although credit institutions are the main issuers of payment accounts, the use of such accounts by payment institutions and electronic money institutions is on the rise, leading to the view that these services present a **significant** residual risk of being misused (abused) for **Money Laundering/Terrorism Financing** purposes.

Despite this risk, since January 2022, Royal Decree-Law 7/2021 of 27 April has introduced the obligation to report payment accounts held by payment institutions and electronic money institutions to the FTF, thereby strengthening the supervision of these institutions through account reporting.

On the other hand, the residual risk associated with payment initiation operations is **moderate to low**, as it relates solely to acting as an intermediary in the payment for goods or services without managing the customer's funds. In other words, once the instruction to initiate the payment has been received, they merely check whether there are sufficient funds in the payer's payment account specified by the payer to proceed with the payment, and, if there are, inform the seller that the payment has been initiated.

As for the activities of account aggregators, their residual risk could be classified as **low**, as they do not act as intermediaries in any payments and merely consolidate information previously analysed by the account managers who, as obliged entities, are subject to the Money Laundering/Terrorism Financing preventive framework. However, these are entities that hold a large amount of aggregated financial information on customers and their funds, and they can play an important role in detecting Money Laundering/Terrorism Financing-related activities that are not detected by the other obliged entities managing the accounts.

Finally, with regard to payment institutions that issue credit and debit cards, their residual risk could be classified as **moderate**, as they generally operate with funds originating from other obliged entities (via direct debits). Nevertheless, as in the previous case, these are entities that hold a great deal of information on customers and the destination or use of their funds, and they can play an important role in detecting Money Laundering/Terrorism Financing-related activities that are not detected by the other regulated entities managing their main accounts.

d) Electronic money transactions.

Activity, context and regulatory framework.

The update to this sector has been prompted by the increase in the number of payment transactions carried out by electronic money institutions. In turn, access to the SNCE and the reporting of payment accounts by this sector to the FTF have facilitated the review of the sectoral risk profile set out below.

Electronic money institutions (EMIs) are those authorised to issue electronic money that is accepted as a means of payment by businesses other than the issuing institution. Electronic money is defined as the monetary value represented by a claim on its issuer. This value, which is stored on an electronic medium, is issued upon receipt of funds in an amount not less than the monetary value issued and is accepted as a means of payment by businesses other than the issuer.

They are regulated by Law 21/2011 of 26 July on electronic money, as amended by Royal Decree-Law 19/2018 of 23 November on payment services and other urgent measures in the financial sector, and its implementing regulations approved by Royal Decree 778/2012 of 4 May.

The process of establishing electronic money institutions requires a number of conditions to be met, such as: a minimum registered share capital of 350,000 euros, a registered office within Spanish territory, and professional and commercial integrity, amongst others. Spanish electronic money institutions must obtain a preliminary report from SEPBLAC assessing the suitability of the proposed governing bodies and procedures, based on the documentation submitted regarding the Money Laundering (ML) and counter-terrorist financing (CTF) structure and procedures they intend to apply once operational.

The procedure for opening branches and providing services freely in Spain by electronic money institutions from other EU Member States is subject to the Banco de España receiving notification from the supervisory authority of the electronic money institution's country of origin.

According to data from the Special Register of Electronic Money Institutions managed by the Banco de España, as of December 2022 there were 13 EMIs registered in Spain. In addition, there are EU-based EMIs that may be operating in Spain without a physical establishment.

EMI institutions share the ability to carry out payment transactions with payment institutions (with the exception of money remittances). Consequently, since December 2021, EMI institutions have been eligible to participate in the SNCE and, pursuant to Royal Decree 7/2021, are required to declare their payment accounts to the FTF.

Financial innovation has contributed to the development of these institutions, improving the level of financial inclusion in society, with some being referred to as the new *'neobanks*'.

Threats.

In their operations, EMIs bear many similarities to payment institutions. Consequently, the threats facing this sector are very similar to those affecting the obliged entities analysed in the previous section. Therefore, the risk of them being used for Terrorist Financing is high, particularly when they act as primary financial institutions in countries with low levels of banking penetration or which are considered high-risk.

It has been established that certain electronic money instruments, such as prepaid cards, have been used in various countries to finance terrorist activities, mainly linked to jihadist groups, due to the absence of customer identification

requirements below certain thresholds. , these instruments are also susceptible to being used by threats originating from third countries where customer identification systems are less rigorous, which has led to an increase in regulatory restrictions in European countries on transactions involving anonymous instruments.

Spanish regulations require customer identification in all cases for transactions involving electronic money, regardless of the amount, although simplified measures are permitted in the following cases:

- Where the electronic money cannot be reloaded and the amount stored does not exceed 250 euros.
- Where, if it can be reloaded, the total amount available in a calendar year is limited to 2,500 euros, except where the holder of the electronic money requests a refund of an amount equal to or greater than 1,000 euros during that same calendar year.

With regard to Money Laundering, the digitalisation of society and the creation of powerful payment platforms by such regulated entities mean that they are being used by criminal organisations and individuals to move funds of illicit origin.

Investigations and strategic reports have revealed the creation of EMI payment accounts for the purpose of moving funds derived from criminal activities carried out by large international organised crime groups whose activities focus on tax fraud. Similarly, intelligence agencies have identified the use of these products for the purpose of channelling funds derived from fraud, human trafficking or drug trafficking.

Vulnerabilities and sector-specific risks.

The potential for the fragmentation of electronic money transactions represents a vulnerability in relation to FT risks, particularly where unlisted parties are involved. The proliferation of online payment platforms that facilitate the acquisition of prepaid cards and international electronic money transfers represents a benefit to society in terms of interoperability, but also a vulnerability in relation to the use of these services for Terrorist Financing and the flows arising from criminal activities committed by criminal groups.

Consequently, the risk of infiltration and activity by organised crime groups is high. Given that the payment institutions sector is subject to very strict controls, there is concern about the high risk of electronic transactions within the e-money sector being used to channel funds linked to Money Laundering and terrorist financing operations.

The **inherent risks** associated with their use for both Money Laundering and terrorist financing purposes are greater than those of other payment systems. This is because these are instruments which, in some countries – though not in the case of Spain – do not provide data on the holders of e-money or on the origin of the funds held (unlike debit or credit cards which, in the case of Spain, contain information on the payer and their linked payment account), do not require the holder of a prepaid card to hold a current account or similar, and allow for their rapid conversion into cash.

The proliferation of this type of service in countries with fewer preventive requirements for obtaining an operating licence from the national authority is a fact. In this regard, the current position of the providers of these services is a cause for concern, as some have come to be regarded as *neobanks* (without holding a banking licence as such).

In Spain, identification is required in all cases at the time of depositing funds, but this identification requirement varies depending on the issuing country, which may set different thresholds; this influences exposure to the risks associated with their potential misuse, both for Money Laundering (ML) and terrorist financing (TF) purposes.

In short, although electronic money offers greater advantages in terms of traceability, the speed of transactions, combined with its global reach and the convenience of accessing online platforms, means that the vulnerabilities associated with this sector in relation to Money Laundering/Anti-Terrorism risk exposure are high.

Conclusion.

The electronic money institution sector faces very high inherent risks that are common across the entire sector. These risks are greater in cases where electronic money is issued in other countries and where controls over the holder's identity and transaction thresholds do not meet the requirements mandated at national level. However, as indicated, the specific regulatory amendments adopted to strengthen the Money Laundering/Terrorism Financing (ML/TF) prevention regime in these institutions, the closer engagement with the sector by regulatory and supervisory authorities, and the increased implementation of internal policies and procedures by institutions in the sector—including improved reporting of suspicious activity—have led to a substantial improvement in the sector's risk profile, which has shifted from 'high' to **'significant'** for both **Money Laundering** and **Terrorism Financing**.

Among the mitigating measures that help to control the EMI sector, it is worth noting that, since January 2022, Royal Decree-Law 7/2021 of 27 April has introduced the obligation to report payment accounts held by payment institutions and electronic money institutions to the FTF, thereby strengthening the supervision of these institutions through account reporting.

(e) Crypto-assets and crypto-asset service providers.

Activity, context and regulatory framework.

The update to this sector has been prompted by the preparation of the Sectoral Risk Analysis of Crypto-Assets (CA) and Crypto-Asset Service Providers (CASP), which has enabled the comprehensive identification of the threats, vulnerabilities and risks affecting the sector.

To date, the only framework applicable to the sector is the preventive one, under which the only crypto-assets subject to regulation are virtual currencies, and the only related services whose providers are considered obliged entities are those involving a) the exchange of virtual currency for fiat currency and b) the custody of electronic wallets.

Notwithstanding the fact that there are currently only two categories of CASP recognised as obliged entities under our legislation, account must be taken of the recent update to the European preventive framework, through the changes already incorporated into Directive 2015/849 by the Funds Transfer Regulation and certain CAs (EU) 2023/1113 of 31 May (hereinafter the 'Funds Transfer and CA Regulation'), which must be implemented in Spain by 31 December 2024. These changes will designate CASP regulated under the Markets in Crypto-Assets Regulation (EU) 2023/1114 of 31 May (hereinafter 'MiCA') as obliged entities, with the exception of those providing advisory services, thereby completing our alignment with FATF standards.

As regards data, there is no certainty regarding the number of active CASP, the full range of networks and CAs with which they operate, or the scope of other services they may provide in addition to exchange and/or custody services. However, a study has been carried out by Chainalysis at the request of COPBLAC, which indicates that amongst the 50 with the highest volume of activity in Spain, the top 10 account for 85.5 per cent of this activity with CAs, and the top three – which represent 60.2 per cent of the activity – are registered with the Banco de España, which mitigates the risk.

This register was established in October 2021 and is a mandatory requirement for all operators wishing to provide this type of service in Spain.

As at 29 June 2023, 76 providers were listed in the Banco de España's Register of Virtual Currency Exchange Service Providers for fiat-to-virtual currency exchange and/or electronic wallet custody; of these, 41 offer exchange services, 4 offer custody services, and 31 offer both. The vast majority are based in Spain, except for 21 which operate under the freedom to provide services.

According to the Global Crypto Adoption Index, which was updated with the June 2023 Report on the State of the Sector in Spain, Spain ranks 34th in terms of adoption levels out of a total of 146 countries. Furthermore, it ranks 99th in terms of P2P transaction volume, indicating that the bulk of activity is concentrated in centralised markets (27th place), where just under two-thirds of CA transactions took place, and decentralised markets (24th place), where adoption is four percentage points above the global average.

However, when placing cryptocurrency transactions in the context of fiat currency activity in Spain, it can be seen that the volume of cryptocurrency transactions, when compared with the value of SEPA transactions (relating to transfers), would account for 5.8 per cent of this activity.

Some of the changes detected by the Spanish authorities, following various falls in the value of cryptocurrencies coupled with factors such as transaction speed and low fees, point to increased use of *stablecoins* (Tether, USDT), which maintain a near-constant value over time relative to the dollar or the euro. According to data provided by Chainalysis regarding inflows and outflows of cryptocurrencies to and from Spain, *stablecoins* are also the dominant form of cryptocurrency, ahead of Bitcoin, Ethereum and other virtual assets[31] .

Threats.

The main threats relating to Money Laundering or Proliferation Financing (hereinafter 'PF') do not generally differ from those in the *fiat* world, but the channelling of funds linked to terrorism, proliferation, extortion, scams, fraud, tax evasion, and drug, arms or human trafficking can prove difficult to trace when the transaction chain involves the use of cryptocurrency exchanges (CA), and even more so when it involves cryptocurrency service providers (CASP) located in non-cooperative jurisdictions or those with more lenient legislation.

According to data from Chainalysis, the volume of CA activity considered high-risk stands at 0.4 per cent (0.6 per cent globally and 0.7 per cent for Western Europe), whilst that considered illicit is estimated at 0.1 per cent (0.4 per cent globally and identical to the European figure).

The main threats in Spain to Terrorist Financing activities stem from the evolution of jihadist terrorism, where operations investigated by the authorities forming part of the LEAs have revealed the use of *privacy coins*. Furthermore, terrorist groups have been found to use *bots* to create numerous addresses, assigning a separate address to each donation and thereby hindering traceability.

Cryptocurrency mining can facilitate the mobilisation of funds by terrorist organisations due to the decentralised nature of cryptocurrencies and the pseudo-anonymity and privacy offered by many of them.

In short, threats linked to terrorism and weapons of mass destruction affect the use of cryptocurrencies for the purpose of channelling funding and purchasing weapons of mass destruction.

With regard to the Money Laundering (ML) unit, the main threats stem from the criminal activities of criminal groups linked to drug trafficking and economic and financial crimes, primarily relating to fraud and corruption. Furthermore, it should be emphasised that, within the context of fraud-related operations, *ransomware* attacks involving cryptocurrencies are one of the main offences identified by LEAs in their investigations.

Vulnerabilities and sector-specific risk.

[31] https://www.guardiacivil.es/es/prensa/noticias/8124.html

For vulnerabilities, see section 5.3.2.

Conclusion.

The inherent risk of **virtual assets or currencies** being used for Money Laundering/Terrorism Financing purposes is **high**. The lack of sufficient applicable regulation, the ease of access to this type of asset, the opacity of their operation and the anonymity of the parties involved, as well as the cross-border nature of the phenomenon, are risk factors that must be taken into account.

However, in Spain, given that the total volume in circulation is low (66.45 billion dollars between March 2022 and 2023), its limited use as a means of payment (accounting for 5.8% of transfers, instant transfers and SEPA transfers) and the fact that the figures for the issuance of digital tokens are very small and subject to supervision by the CNMV, the actual risk of their use for Money Laundering/TF purposes should be considered mitigated in relation to the high inherent risk.

Taking all this into account, **virtual currencies** pose a **significant/moderate** residual risk in terms of their use in both Money Laundering and Terrorism Financing activities; this assessment is based on their limited use and on the investigations carried out to date, which have analysed the use of virtual currencies and assets for these purposes. However, it should be reiterated that the difficulty involved in detecting and monitoring these transactions has only allowed for the identification of isolated cases and that, so far, the figures involved have been of little significance.

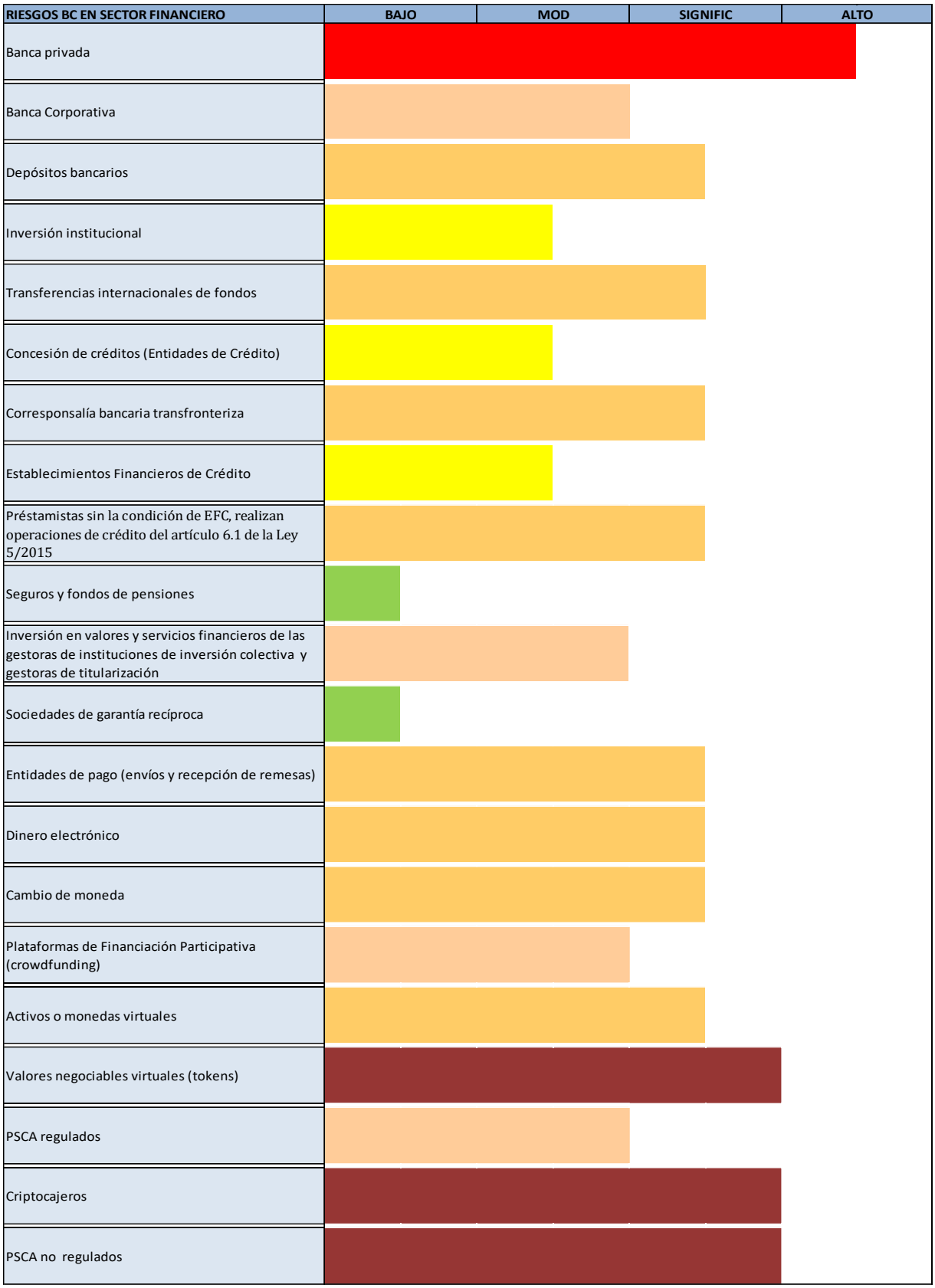
These risks are lower for the use of **virtual transferable securities (tokens)**: although they pose a **significant** risk in relation to Money Laundering (ML) activities, the residual risk should be considered **moderate** for terrorist financing (TF) and Proliferation Financing, as the very nature of this type of investment service is linked to the potential financial return on products, which entails greater management complexity and lower risk exposure when used for the purposes of TF and Proliferation Financing.

Regulated CASP in Spain pose a **significant** inherent risk in relation to Money Laundering/Terrorism Financing (ML/TF); this assessment is based on the type of services they provide, non-face-to-face relationships, their operations and the existence of unregistered regulated CASP, and their residual risk is **moderate**, whilst the residual risk for ***crypto ATMs*** remains **significant**.

Unregulated CASP in Spain pose a high inherent risk in relation to Money Laundering/ FT, due to the nature of their operations, given that they are not limited to custody services and the exchange of cryptocurrency for fiat currency, but also encompass activities involving CA, in which risks may be heightened due to their transactional nature, *cross-border nature* and a lack of understanding regarding the application of national AML/CFT measures. Their residual risk is **significant**, mainly due to the proportion of activity carried out by three CASP entities that are registered with the Banco de España.

Money Laundering RISK TABLE: FINANCIAL SECTOR[32]

[32] The table contains all the information on all the sectors analysed in the 2020 NRA, not just those amended in this addendum.



FINANCIAL SECTOR ML RISK TABLE[33]

[33] The table contains all the information on all the sectors analysed in the 2020 NRA, not just those amended in this addendum.


RIESGOS FT EN SECTOR FINANCIERO
BAJO
MOD
SIGNIFIC
ALTO
Banca privada
Banca Corporativa
Depósitos bancarios
Inversión institucional
Transferencias internacionales de fondos
Concesión de créditos (Entidades de Crédito)
Corresponsalía bancaria transfronteriza
Establecimientos Financieros de Crédito
Préstamistas sin la condición de EFC, realizan operaciones de crédito del artículo 6.1 de la Ley 5/2015
Seguros y fondos de pensiones
Inversión en valores y servicios financieros de las gestoras de instituciones de inversión colectiva y gestoras de titularización
Sociedades de garantía recíproca
Entidades de pago (envíos y recepción de remesas)
Dinero electrónico
Cambio de moneda
Plataformas de Financiación Participativa (crowdfunding)
Activos o monedas virtuales
Valores negociables virtuales (tokens)
PSCA regulados
Criptocajeros
PSCA no regulados

f) Use of cash, cash flows and cash-intensive businesses.

Activity, context and regulatory framework.

The update to this sector has been prompted by regulatory changes regarding the reporting of payment flows, which bring Spanish regulations into line with the provisions set out in Commission Implementing Regulation (EU) 2021/776 of 11 May 2021. Furthermore, account has been taken of the widespread use of cash in Spanish society; according to the Banco de España's *2022 Study on Cash Usage Habits*, cash is currently considered the primary method of payment in Spain.

As described in the chapter on vulnerabilities, cash transactions are very common in Spain, with cash being the most widely used payment method; and although other forms of transaction are becoming increasingly widespread, a significant number of cash transactions are still carried out involving private individuals and, to a lesser extent, businesses.

These transactions and the physical movement of cash have been progressively restricted in Spain. Movements of payment instruments have been the subject of considerable attention from the perspective of Money Laundering and terrorist financing (ML/TF) prevention, and evidence of the use of large amounts of cash in criminal schemes has led to greater restrictions and controls on its use since 2003, the year in which the legal framework governing capital movements and economic transactions with foreign countries, as well as certain ML prevention measures, was adopted.

The need to control movements of payment instruments has been reaffirmed at European level by various regulations concerning controls on the entry or exit of cash from the Union, progressively increasing existing obligations and coordination between Member States. Regulation (EU) 2018/1672 extended these obligations to gold, prepaid cards and cash sent by post or transported as goods or via courier services. If cash is sent by other means (unaccompanied cash), the competent authorities shall be empowered to require the sender or recipient to make a declaration disclosing the relevant information and to carry out checks on any consignment, parcel or means of transport that may contain cash.

With a view to standardising declarations of cash movements across Europe, Commission Implementing Regulation (EU) 2021/776 of 11 May 2021 established the templates for certain forms, as well as the technical standards for the effective exchange of information pursuant to Regulation (EU) 2018/1672 of the European Parliament and of the Council on controls on cash entering or leaving the Union. This Regulation was supplemented at national level by Order ETD/1217/2022 of 29 November, which regulates declarations of movements of means of payment in the context of the prevention of Money Laundering and terrorist financing.

At national level, persons carrying out movements of means of payment are required to make a declaration when such movements reach or exceed 10,000 euros when entering or leaving Spain, or 100,000 euros when moving within the national territory. In the case of movements within the national territory or of movements into or out of the national territory of accompanied means of payment, originating from or destined for a Member State, such declarations must be made using form S1 (if unaccompanied, the declaration is made using form S2). In the case of movements into or out of Spain of accompanied means of payment originating from or destined for a third country, Form E1 must be submitted (if unaccompanied, the declaration is made using Form E2).

Declarations relating to movements of means of payment exceeding 100,000 euros within Spain increased considerably in 2020 compared with previous years. However, the figures for 2021 and 2022 are similar to those from the pre-pandemic period, confirming that the use of cash as a legitimate means of payment is declining due to the progressive prevention and control measures adopted at national level in relation to payments made in this way.

Meanwhile, cross-border payment transactions declined during the pandemic years, falling by 64 per cent in 2020 and 57 per cent in 2021. In 2022, this figure has increased considerably, with the number of declarations now at levels similar to

those of 2019, whilst the amounts declared on entry show a rise of 143 per cent and those on exit a rise of 125 per cent compared with that year.

Furthermore, Article 27.1 of Royal Decree 304/2014 of 5 May, which approves the Regulations of Law 10/2010 of 28 April, establishes the obligation for credit institutions to report to SEPBLAC, on a monthly basis, the number and value of transactions involving cash movements exceeding 30,000 euros without being credited to or debited from the customer's account; furthermore, it stipulates that regulated entities must report money transfer transactions on a monthly basis.

Furthermore, tax legislation has tightened restrictions on cash payments in view of the close link between the use of cash and economic crimes, and its potential use for Money Laundering and terrorist financing purposes. Thus, the limit on cash payments has been reduced from 2,500 to 1,000 in the case of commercial transactions and from 15,000 to 10,000 euros where one of the parties is a non-resident and is not acting in a business or professional capacity, which has undeniable effects on preventing the use of cash for Money Laundering purposes.

Threats.

The link between cash and certain **threats** arising from organised crime and Terrorist Financing is evident, given the characteristics of cash that facilitate the misuse of cash movements for criminal purposes. Consequently, there is evidence of networks involved in smuggling, drug trafficking, sexual offences, human trafficking, the smuggling of illegal goods, fraud and scams, etc., which carry out their criminal activities largely through cash transactions, as this is the only way to ensure that the funds cannot be traced by the authorities responsible for investigating and combating such behaviour.

Vulnerabilities and risks.

The risks inherent in the movement of cash and its potential use for Money Laundering/Terrorism Financing purposes are very high. As already noted when analysing its vulnerabilities as a means of payment, the widespread use of cash in our country poses a significant risk of it being used for illicit purposes. Anonymity and the lack of traceability of funds prevent verification of their origin (lawful or unlawful), allow them to be transferred to third parties for unlawful purposes, enable their laundering through the integration of such funds into the financial system, the acquisition of other illicit goods, or the carrying out of criminal activities.

Inherent risks of Money Laundering. The inherent risks associated with the use of cash in Money Laundering are very high (the use of 50-euro notes is very common). Restrictions, greater awareness amongst financial institutions and other regulated entities regarding the use of cash for Money Laundering purposes, and the growing difficulties in depositing cash into the national financial system are leading to a decline in its use as a means of payment. These measures also contribute to greater concealment and the outflow of large amounts of cash to third countries via various mechanisms, generally using **high-denomination banknotes**, as these offer an advantage in terms of storage and transport, taking up less space and being easier to conceal.

This **cross-border movement** of funds makes it very difficult for the authorities to trace the proceeds of crime and identify evidence of their illicit origin; furthermore, it allows the process of laundering those funds to be carried out more easily in another country where there is no evidence or suspicion that the cash is the proceeds of an unlawful act. Even if the cash is detected in the destination country, the legal and practical implications can thwart efforts to prosecute offenders and confiscate the cash.

On other occasions, funds derived from crimes committed abroad or committed in Spain and subsequently transported abroad are brought into our country with the aim of using them under the guise of legality (for example, by pretending they are income from commercial activities).

The EU SNRA report also highlights the appeal of cash movements for criminal organisations seeking to launder money of illicit origin. Generally, these individuals carry smaller amounts that are more difficult to detect and may not be subject to the declaration requirement applicable to individuals carrying 10,000 euros or more.

These risks associated with the use of cash for Money Laundering purposes have also been identified in **businesses where cash is used more extensively**, as such entities or professions may be exploited by criminal networks to launder cash of illicit origin by mixing it with cash of licit origin that enters these businesses. Despite the existing limits on the use of cash in commercial transactions (1,000 euros) described in this section, and the awareness among the authorities and the financial sector of such practices, the risk of illicit cash entering the financial system via these businesses remains high.

Inherent risks of Terrorist Financing. As already noted, the special characteristics of cash (anonymity, ease of transport, lack of traceability, etc.) make it a key element in Terrorist Financing activities.

Cash funds are used to finance individual terrorists and terrorist groups, their cells, their day-to-day living expenses (accommodation, transport, food, etc.), their activities (indoctrination, training, propaganda, use of social media, etc.), their support networks and, of course, the acquisition of weapons and materials for terrorist activities.

As with Money Laundering, the movement of cash is of enormous significance, although detecting them is even more complex because, on the one hand, as has been highlighted, the **sums involved in terrorist financing are much lower than those for Money Laundering** and even fall below the international thresholds for reporting such movements (generally 10,000 euros) and, on the other hand, because the funds intended for terrorist financing sometimes have a legitimate source.

Similarly, as the EU's SNRA also highlights, it has been demonstrated that terrorist groups have used various techniques to move cash across external borders, particularly in the case of larger organisations. This threat is particularly significant with regard to movements from the EU to third countries. Furthermore, cases have been identified in which foreign terrorist fighters have acted as cash couriers to finance their travel and stays in conflict zones.

With regard to **businesses where there is greater use of cash**, cases have been detected of such entities being used for the purposes of terrorist financing, and although this type of financing system requires greater technical expertise to conceal funds from different sources and involves initial investment costs, the level of risk is still considered to be significant.

Residual Money Laundering and TF risks.

Awareness of the high risk associated with the use of cash has led to the establishment of certain regulatory restrictions to control its use, which are enforced by both the authorities and the private sector. Among other measures, the following are worth noting:

- Individuals are legally obliged to submit an administrative declaration when carrying out physical movements of cash (or other means of payment), whether within the national territory (€100,000) or when crossing Spanish borders (€10,000).
- Between 2019 and 2022, an annual average of 12,764 declarations of cash movements across borders were received (amounting to an annual average of 754 million euros), and 2,970 declarations of cash movements within the country (amounting to an annual average of 573 million euros).
- A limit is imposed on cash payments of 1,000 euros or more where one of the parties is acting in a business or professional capacity, in addition to payments or deposits made at credit institutions, and on payments of 10,000 euros or more where one of the parties is a non-resident.
- There is an obligation to declare cash deposits and withdrawals at credit institutions amounting to 100,000 euros or more (or the equivalent value in foreign currency). Between 2019 and 2022, there was an annual average of 8,531 cash deposits and withdrawals amounting to 100,000 euros or more.

- Funds subject to administrative declaration at the border because they exceed 10,000 euros and which are not declared will be automatically seized. This is carried out by customs or police officers when verifying compliance with the declaration obligation. Between 2019 and 2022, an annual average of over 14 million euros was seized due to this failure to declare.
- Failure to comply with the legal declaration obligations gives rise to the initiation of the relevant penalty proceedings, with the corresponding fines being imposed. Between 2019 and 2022, the average annual number of penalties imposed for such breaches stood at 367 per year.
- Regulated entities must report monthly the number and value of transactions involving cash movements exceeding 30,000 euros without a credit or debit to the customer's account. This obligation applies to regulated entities carrying out cash remittance transactions for amounts exceeding 1,500 euros. In the period 2019–2022, the average annual number stood at 588,500 transactions.

CUADRO 10. Datos sobre movimientos de efectivo

Movimientos de medios de pago por territorio nacional iguales o superiores a 100.000 €

	2018	2019	2020	2021	2022
Movimientos de medios de pago por territorio nacional (con declaración) *					
Nº operaciones	2.530	2.744	4.187	2.380	2.570
Importe total (€)	482.567.654	546.130.748	758.524.056	459.119.478	528.663.055
Actas de intervención dentro de España (sin declaración)					
Nº de intervenciones	33	27	50	41	33
Cuantías intervenidas (€)	5.175.824	7.325.673	12.909.148	10.936.880	10.499.225
Cuantías confiscadas (€) (por sanción)	3.753.554	2.854.354	1.992.823	4.455.293	3.917.089

Fuente: SEPBLAC y SGICMC

Movimientos de efectivo en frontera superiores o iguales a 10.000 €

Declaraciones por movimiento de medios de pago en efectivo en frontera por importe superior o igual a 10.000 €	**2018**	**2019**	**2020**	**2021**	**2022**
Nº operaciones de entrada	7.629	8.060	2.892	3.442	7.202
Importe total (€)	337.308.112	359.732.062	146.051.168	217.257.843	873.001.186
Nº operaciones de salida	9.274	9.945	5.228	5.636	8.649
Importe total (€)	304.678.831	310.924.046	151.995.938	257.772.104	699.665.723

Fuente: SEPBLAC

Actas de intervención en frontera por importe superior o igual a 10.000 euros (sin declaración)

	2018	2019	2020	2021	2022
Nº actas por infracción	**459**	**484**	**301**	**342**	**341**
Nº entradas	152	143	155	195	191
Nº salidas	307	341	146	147	150
Cuantías intervenidas (€)	19.256.280	23.077.088	11.897.015	7.161.058	15.255.694
Cuantías confiscadas (€) (por sanción)	9.890.480	7.536.095	5.556.782	4.703.538	3.329.212

Fuente: SEPBLAC

Conclusion.

As indicated, cash movements carry very **high** inherent risks in relation to Money Laundering/Terrorism Financing. However, there is a high level of expertise in this field, which has for years led to comprehensive regulation, monitoring and sanctions in the area of Money Laundering/Terrorism Financing prevention: sectoral risk analyses and the statistical data collected have made it possible to identify patterns, the main geographical points of entry into and exit from the country, profiles (differentiated by entries and exits, by geographical location…), preferred destinations, routes taken, most commonly used currencies, etc. This has enabled the customs and police authorities to become increasingly specialised and to adopt measures targeted at the greatest risks identified, as well as control measures aimed at ensuring the correct taxation arising from the ownership and transfer of virtual currencies and the origin of the funds used to acquire them.

The alignment of Spanish legislation with European regulations, combined with the additional declaration requirements in force in our country and the high level of national cooperation and oversight by the customs services, has contributed to a continuous reduction in the risk of these activities being used for Money Laundering operations, which involve both the movement of cash and businesses with a high volume of cash transactions; various measures have been adopted in this regard.

Cash movements. Despite the numerous measures adopted and the resources deployed, the number of travellers crossing Spain's borders is very high, as is the potential volume of funds being transported; this, combined with the risks inherent in cash (anonymity, lack of traceability, ease of transport, etc.), justifies the view that the **residual risk** to **Money Laundering** and **FT** from cash movements continues to be considered **high**.

Businesses that routinely handle cash. Owing to the inherent risks associated with cash, as noted above, the risk of cash of illicit origin entering the financial system via businesses that routinely handle cash for **Money Laundering** purposes is **significant/high**. However, in the case of **terrorist** financing, due to the circumstances outlined above, this risk is lower than that associated with cash movements, but still significant enough to be regarded as **substantial**.

TABLE: ML RISKS ASSOCIATED WITH CASH MOVEMENTS

RIESGOS BC EN USO DE DINERO EN EFECTIVO	BAJO	MOD	SIGNIFIC	ALTO
El uso de dinero en efectivo				
Negocios con uso habitual de efectivo				

TABLE: ML RISKS ASSOCIATED WITH CASH MOVEMENTS

RIESGOS FT EN USO DE DINERO EN EFECTIVO Y DE MONEDAS VIRTUALES	BAJO	MOD	SIGNIFIC	ALTO
El uso de dinero en efectivo				
Negocios con uso habitual de efectivo				

8.2. Risk in non-financial sectors .

(a) Activities carried out by notaries.

Activity, context and regulatory framework.

The review of this sector has been prompted by the creation of the Central Register of Real Property Ownership through Royal Decree 609/2023 of 11 July, which also approves its operating Regulations. Furthermore, supervisory measures have been carried out which have highlighted the threats and risks affecting this sector.

A notary is a public official of the State, appointed following a competitive examination, whose role is to provide citizens with the legal certainty enshrined in the Constitution in the field of extrajudicial legal transactions. They are legal professionals practising on a competitive basis, although their fees are standardised across the profession. As at 31 December 2022, there were some 2,691 practising notaries in Spain, organised into 17 notarial associations and spread throughout the country. The notarial associations support them in their role and oversee their conduct. The deans of these associations form the General Council of Notaries, which represents the profession at national level. Notaries report hierarchically to the Directorate-General for Legal Certainty and Public Trust within the Ministry of the Presidency, Justice and Relations with Parliament.

Law 10/2010 of 28 April stipulates that notaries are obliged entities; however, notarial and registration acts that lack any financial or asset-related content, or which are not relevant for the purposes of preventing Money Laundering and terrorist financing, are not subject to these obligations.

In the exercise of their preventive obligations regarding Money Laundering/Terrorism Financing, pursuant to Article 27 of Law 10/2010 of 28 April, Article 44 of its Regulation stipulates the necessary inclusion of notaries within the Centralised Prevention Body (OCP). The purpose of establishing the OCP is to intensify and strengthen collaboration between members of the notarial profession and the judicial, police and administrative authorities, thereby enabling a higher level of specialisation in these tasks amongst the group of obliged entities. Its creation pursues a twofold objective:

- To facilitate compliance by individual notaries with preventive regulations, by providing a specialised body responsible for administrative and procedural functions which also channels reports of suspicious transactions, thereby improving their quality and speeding up the process.
- To standardise the measures applied by the profession, thereby avoiding potential differences of interpretation regarding the scope and meaning of the obligations.

The Centralised Money Laundering Body of the General Council of Notaries was established in December 2005 as a direct result of the publication of Order EHA/2963/2005 of 20 September. As indicated above, membership is compulsory for notaries.

The General Council of Notaries maintains the Single Computerised Notarial Register, in which notarial acts are recorded. The OCP of the General Council of Notaries has access to this register.

Notaries have access to an extensive database on real property ownership, to which the AEAT was granted access in 2021 through the signing of an agreement to strengthen the fight against tax fraud.

Furthermore, Royal Decree 609/2023 of 11 July established the Central Register of Real Property Ownership and approved its operating regulations. This Register incorporates, amongst other sources, the information contained in notarial databases.

In accordance with the provisions of Law 11/2023 of 8 May on the digitisation of notarial and registry procedures, since 9 November 2023, notaries have been able to provide certain notarial services remotely, primarily of a commercial nature. These include corporate acts, commercial deeds, various types of powers of attorney, letters of payment, cancellation of guarantees, certificates of legitimacy, wills drawn up during an epidemic and, in some cases, settlements and legal acts and transactions, amongst others. The procedures are carried out via the notarial electronic portal, using videoconferencing and advanced electronic signatures. The sector estimates that more than 3,200,000 notarial documents could be authorised and signed via notarial channels each year.

Threats.

The risk of Money Laundering in notarial transactions is linked to the fact that virtually all property and commercial transactions must be witnessed or authorised by a notary and, as is the case with other public notaries, to the appearance of legality that public deeds confer on the property and assets included therein in favour of those seeking to obtain the use of property acquired with illicit funds.

Bearing in mind that the aim of all types of threats is to secure the formal legitimacy of transactions conferred by public institutions, the role of notarial deeds is key within this process of concealing illegality.

Furthermore, the establishment of companies controlled by terrorist organisations or for the purpose of mobilising funds whose ultimate aim is to finance these groups is one of the main threats in the field of Terrorist Financing.

The same applies to Money Laundering and the abuse by criminal organisations of the notarial function in order to carry out the crimes for which they were established.

The creation of corporate structures where beneficial ownership cannot be properly identified due to the presence of trusts and frontmen in corporate transactions or property sales represents the main threat to efforts to combat organised crime.

Vulnerabilities and sector-specific risk.

The factors that make the notarial sector vulnerable to Money Laundering/Terrorism Financing risks stem from its own activities, particularly in the following areas:

- The incorporation of companies, particularly limited liability companies, and the transfer of shares in such companies.
- The sale and purchase of real estate.

On occasion, different notaries may be involved in several interlinked notarial acts. This factor makes it difficult to gain a complete overview of the transaction, thereby increasing the sector's vulnerabilities in such cases.

Notaries are obliged to abstain, in accordance with Article 19 of Law 10/2010 of 28 April, in accordance with the terms set out in paragraph 2 of that article*: "For the purposes of this Law, just cause justifying the notary's refusal to authorise a transaction or their duty to abstain shall be understood to mean the presence in the transaction of either several risk indicators from among those identified by the centralised prevention body, or clear evidence of simulation or fraud." To this end, and without prejudice to the provisions of Article 24, the notary shall obtain from the client the information necessary to assess the presence of such indicators or circumstances in the transaction".*

The endogenous risk of such practices infiltrating the notarial sector is low due to the specialised nature of entry into the profession and the conditions governing its practice. However, the exogenous risk factor of the misuse of notarial services

for these purposes is very high. These risks stem from criminals' need and ability to feign, before the notary, the legitimacy of the transactions they intend to carry out and the origin of the funds used in those transactions, with the ultimate aim of obtaining a notarial deed that lends an appearance of legitimacy to their ownership of property or assets.

This Money Laundering/Terrorism Financing (ML/TF) risk in notarial transactions can be identified through a series of risk indicators, defined by the OCP, which are simply factual circumstances that experience has shown to be associated in practice, primarily, with Money Laundering schemes, as revealed by court rulings, the OCP's own risk analysis or the classification exercises carried out by international organisations.

Of the nearly 400 different types of transactions carried out by notaries, the incorporation of companies and transfers of ownership, together with property sales, account for the greatest proportion of the risk, as we have mentioned previously. This risk is quite significant, whether we are referring to transactions reported by notaries on the basis of suspicion or to those analysed and forwarded to SEPBLAC by the Notarial OCP, given that these notarial acts account for 15 per cent of the activity carried out by notaries and 51 per cent of the reported transactions relate to this category.

Alongside the two transactions mentioned above, the three highest-risk Money Laundering transactions – which, when added to the previous two, would account for more than 70 per cent of all reported high-risk transactions – are:

- Company capital increases.
- Loans and acknowledgements of debt.
- Notarisation deeds.

In general, there is a considerable degree of correspondence between the types of high-risk transactions identified by notaries and those ultimately reported by the OCP to SEPBLAC. However, there are cases in which the significance of certain transactions increases following the OCP's analysis of the circumstances identified by the notary. The most striking example concerns notarisation deeds, in respect of which the OCP assesses a significantly higher level of money laundering risk than that typically perceived by notaries.

With regard to risk indicators, the levels generally remain the same as for transactions. However, the proportion of some of the indicators increases following a specific review by the OCP, as in the case of the two indicators involving the presence of a high-risk territory (party involved and source of funds). The same situation applies to the involvement of individuals reported to have participated in criminal activities, as a result of the additional investigation carried out during the ex-post analysis phase by the OCP.

A general analysis of the risks associated with transaction types and indicators reveals the following:

- The sale and purchase of property carrying the highest level of risk occurs in cases involving persons or funds from high-risk territories, whether carried out between parties with some form of connection, or where significant discrepancies are observed in the declared price; as well as sales and purchases in areas of Spain where there is known to be intensive use of cash.
- The highest-risk sales and purchases of shares are those in which the price is considered abnormally low or those taking place within a group or sequence of transactions without any particular logical economic or commercial explanation. The highest level of risk associated with company incorporations usually arises when multiple pre-established companies are involved or, in particular, when the founder uses them for other purposes.
- In the case of capital increases, the highest risk arises when funds or assets originating from high-risk territories are used, or when such contributed funds or assets do not correspond to the characteristics of the company increasing its capital, or are difficult to value or verify, particularly in the case of contributions of claims against third parties or the company itself, and in the contribution of shares or holdings in companies from third countries.
- In the case of financing transactions (loans and acknowledgements of debt), the highest level of risk stems from the involvement of individual lenders other than credit institutions, and from instances where the same (private) lender or borrower is repeatedly involved in several transactions within a short period of time.

- It should be emphasised that transfers of shares in limited liability companies (S.L.) carried out by private deed and abroad fall outside the control of notaries, although in such cases notarisation takes place at the relevant consular offices and the associated risks are being mitigated through the agreement signed in 2020 for their monitoring by the OCP.
- Transfers of shares in public limited companies that do not have their private agreement notarised are also outside the scope of notaries' authority.

Conclusion.

Their status as public notaries, whose involvement is essential in numerous types of transactions, means that attempts by third parties to use them to legalise Money Laundering operations are inevitable. Their role in economic life is very significant, as the vast majority of property transactions and corporate operations require their involvement. The risk of Money Laundering/Terrorism Financing (ML/TF) is higher in certain types of transactions: transfers of shares in limited liability companies; sales of property; company capital increases; and loans/acknowledgements of debt.

Notaries in Spain have developed an advanced Money Laundering/Terrorism Prevention detection system following the establishment of the Centralised Prevention Body within the General Council of Notaries, which employs highly sophisticated tools, such as the Single Computerised Notarial Index, which cross-references information from millions of notarised transactions across the country—all of which are duly analysed by the OCP's specialist team—or the Beneficial Ownership Database, which enables notaries, authorities and regulated entities to verify the accuracy of declarations regarding the ultimate beneficial owners of legal entities carrying out transactions subject to a public deed.

These highly developed tools, combined with the high level of knowledge and awareness amongst professionals – which has made this one of the sectors reporting the highest number of transactions to SEPBLAC on the basis of suspicion – enable the residual risk to be significantly reduced. For these reasons, and due to the very nature of the transactions subject to notarisation, the residual risk of these transactions being used for **money laundering purposes** is assessed as **low/moderate**.

However, this risk is higher in certain types of transactions: transfers of shares in limited liability companies; sales of immovable property; company capital increases; and loans/acknowledgements of debt. These transactions account for a significant proportion of the notarial profession's caseload, which is why the residual risk in **Money Laundering** is classified as **moderate**.

b) Activities carried out by land, commercial and movable property registrars.

Activity, context and regulatory framework.

The modernisation of this sector has been driven by the creation of the Central Register of Real Property Titles through Royal Decree 609/2023 of 11 July, which also approves its operating Regulations.

Property, commercial and chattel registrars are civil servants of the State who are appointed to their posts through competitive examinations and whose role is to maintain the property, commercial and chattel registers existing in Spain. Registrars shall, under their own responsibility, assess the legality of all types of documents on the basis of which registration is sought. For documents to be entered in the relevant registers, the registrar must give a favourable assessment.

Under the law, only documents formalised by a notarial deed or a judicial or administrative decision may be entered in the register; consequently, any registration procedure requires the prior involvement of a notary, a judge or an administrative authority, subject to the exceptions laid down by law. This is the general rule in Land Registries and Commercial Registries, although there are also cases where private documents are entered in the register, albeit rarely in Land Registries (in cases involving sole heirs or the distribution of mortgages) or more commonly in Commercial Registries (the appointment and removal of directors, or the appointment of auditors). Meanwhile, in the Registers of Movable Property, the general rule is that entries are made on the basis of private documents (approved model finance lease agreements).

In Spain, there are 1,078 registrars (2022), who receive their fees in accordance with the scale of charges approved by the Ministry of the Presidency, Justice and Relations with Parliament, which also covers the costs necessary for the operation and maintenance of the registers. Registrars do not operate on a competitive basis, but rather on the basis of territorial jurisdiction; consequently, citizens do not have freedom of choice regarding which registry to use. This unique feature provides an additional safeguard, as registrars are not subject to market forces in the performance of their duties, which has a positive effect on the prevention of Money Laundering and terrorist financing.

In carrying out their preventive duties regarding Money Laundering and terrorist financing—as also mentioned in the analysis of notaries—Law 10/2010 of 28 April provides for the possibility of establishing centralised prevention bodies for the regulated professions. The creation of a centralised prevention body aims to intensify and strengthen collaboration between members of professional bodies and the judicial, police and administrative authorities, enabling a higher level of specialisation in these tasks within the group of obliged entities. Its creation pursues a twofold objective:

- To facilitate compliance by individual regulated professionals with preventive regulations, by having a specialised body responsible for administrative or procedural functions which also channels reports of suspicious activity, improving their quality and speeding up the process.
- To standardise the measures applied by the sector, thereby avoiding potential divergent interpretations regarding the scope and meaning of the obligations.

The centralised anti-money laundering body for registrars, established in 2015, is known as the Anti-Money Laundering Registry Centre (CRAB), and registration with it is mandatory.

In 2018, a Ministerial Order established the forms for the submission of annual accounts of commercial companies to the Commercial Register, requiring the mandatory declaration and updating of their beneficial ownership, which is subject to registration in the Beneficial Ownership Register (RETIR). This system has a very positive impact on national systems for monitoring beneficial ownership and on the level of awareness amongst the authorities and obliged entities, in line with national and international requirements for combating Money Laundering and terrorist financing.

Royal Decree 609/2023 of 11 July, which establishes the Central Register of Beneficial Ownership and approves its Regulation, imposes obligations on registrars to verify the identity of the beneficial owner. Consequently, when carrying out their registration duties, registrars must consult this register in order to fulfil this obligation.

Due diligence obligations are further reinforced by the recent amendment to the Third Additional Provision of Law 10/2010 of 28 April, pursuant to Royal Decree-Law 5/2023 of 28 June, which stipulates that obliged entities may not rely solely on the information contained in the RCTIR, but must carry out additional checks, except in the case of business relationships or customers subject to simplified due diligence measures, and provided that the information obtained is reasonably satisfactory and does not give rise to suspicion.

Threats.

The Money Laundering risk in registration transactions stems from the fact that the registration procedures carried out by these obliged entities are, in practice, largely based on the formal legality of the documents drawn up by professionals in this sector.

The registration of commercial transactions involving companies incorporated in high-risk or offshore jurisdictions which are also held in trust poses a threat to the system, as there is a risk that they may be controlled by terrorist organisations or created for the purpose of moving funds intended to finance such organisations.

The same applies to Money Laundering and the abuse by criminal organisations of the registration function to facilitate the commission of the offences for which they were established.

The establishment of corporate structures where beneficial ownership cannot be properly identified due to the presence of trusts poses the main threat to efforts to combat organised crime.

Vulnerabilities and sector-specific risks.

The public faith placed in registrars is safeguarded by the courts, subject to the principle of legitimation, whereby the holder of the registered right is presumed to be the owner vis-à-vis third parties – a situation highly coveted by those seeking to enjoy the use of property acquired with illicit funds. The ultimate aim of Money Laundering activities is to ensure that property and assets derived from illicit activities acquire the formal legitimacy conferred by public institutions; consequently, the role of entries in public registers is key to this process of concealing the origin of assets and creating the appearance of legitimacy.

There is no **endogenous risk** of infiltration within the sector due to the specific nature of the system governing entry into the profession and the conditions regulating its practice. However, this function of public faith, publicity and guarantee vis-à-vis third parties means that the **exogenous risk** of criminal organisations abusing registration services for these purposes is high.

Consequently, the **inherent risks** stem from the actions of criminals seeking to give the appearance of legitimacy to the property and commercial transactions they intend to carry out, and from the origin of the funds used to carry out these transactions, with the ultimate aim of securing registration that confers formal validity vis-à-vis third parties. The main transactions subject to risk in registration procedures are similar to those identified in the analysis at regarding notarial activities (property sales, transfers of company shares, loan transactions, etc.).

For these reasons, in Spain, as in the rest of Europe, registrars are legally designated as obliged entities in the field of Money Laundering/CFT, despite not being among the professions designated by the FATF. Their preventive functions, coordinated through the CRAB Anti-Money Laundering Registry Centre, play a very significant role within the national prevention framework, significantly reducing the inherent risks associated with registry activities.

There are, therefore, numerous mitigating factors: entry to the profession via a competitive examination, which guarantees a high standard of legal training; the fact that they do not operate in a competitive market; the existence of the CRAB, which specialises in anti-money laundering and coordinates preventative policies, risk identification and the reporting of suspicious transactions; and the assessment of legality carried out by registrars when evaluating judicial, administrative, notarial and private documents intended for registration.

Conclusion.

The professional duties assigned to them, the legal obligation to register certain transactions, and the legal certainty afforded by the register for both commercial and property transactions mean that the involvement of registrars is essential

to obtain the presumption of legality reflected by the register itself, which inevitably has an impact on risk from a Money Laundering/CFT perspective.

However, the specific entry requirements for the profession and the strict regulation and conditions governing its practice rule out any inherent risks of attempts to involve the sector in Money Laundering/Terrorism Financing schemes. Furthermore, as regulated entities, they have established a centralised prevention body, the CRAB, which provides the entire professional body with a highly advanced prevention system.

The obligation to file beneficial ownership information with the Commercial Register alongside the filing of annual accounts, and the existence of the Register of Beneficial Ownership (RETIR), which is maintained by commercial registrars, provides automated access to data on company ownership in a structured format; this data is, in turn, used by public authorities and regulated entities. Furthermore, Royal Decree 609/2023 of 11 July, which establishes the Central Register of Beneficial Ownership and approves its operating Regulation, imposes obligations on registrars to verify the identity of the beneficial owner. This legislation reinforces compliance with due diligence measures in this sector.

Finally, all natural or legal persons who, in a business or professional capacity, provide services classified as corporate services (or corporate services provided by third parties) are required to register with the Commercial Register competent for their place of domicile, in accordance with the Commercial Register Regulation.

FT risks. The involvement of registrars in certain transactions and certain types of business that could be used for FT activities has an impact on FT risk. However, the types of transactions that must be registered do not currently correspond to the FT risk profile in our country; therefore, in general, the level of residual risk is considered to be **low/moderate**.

Money Laundering (ML) Risks. The risk is higher for money laundering operations due to certain types of high-risk transactions: sales of real estate, loans/acknowledgements of debt, and corporate transactions of various kinds, such as capital increases and the transfer of shares (an act which has not been recorded in the Commercial Registers since 1995, being reflected solely in the private registers of shares and holdings maintained by companies, with access restricted to shareholders). All of these are routine transactions in the course of professional practice, which is why the residual risk associated with their use is classified as **moderate**.

TABLE: Money Laundering RISKS IN NON-FINANCIAL SECTORS[34]

[34] The table contains all the information on all the sectors analysed in the 2020 NRA, not just those amended in this addendum.

RIESGOS DE BC SECTORES NO FINANCIEROS	BAJO	MOD	SIGNIFIC	ALTO
Giros en servicios postales				
Intermediarios en concesión de crédito				
Operaciones en el sector inmobiliario				
Asesores fiscales y contables externos				
Auditores externos				
Notarios				
Registradores				
Procuradores				
Actividades del Art. 2.1.ñ) Ley 10/2010 realizadas por abogados y otros profesionales				
Prestación de servicios societarios				
Transmisión de sociedades preconstituidas				
Casinos				
Loterias				
Apuestas mutuas deportivas benéficas (quinielas)				
Operaciones de juego presencial: bingos y máquinas tipo B				
Operaciones de juego presencial: apuestas deportivas				
Apuestas deportivas online				
Otros juegos online				
Consursos				
Compra-venta de joyas, piedras y metales preciosos				
Arte y antigüedades				
Comercio profesional de otros bienes de alto valor				
Inversión en bienes tangibles				
Transporte de fondos				

TABLE: FT RISKS IN NON-FINANCIAL SECTORS[35]

RIESGOS DE FT SECTORES NO FINANCIEROS BC	BAJO	MOD	SIGNIFIC	ALTO
Giros en servicios postales				
Intermediarios en concesión de crédito				
Operaciones en el sector inmobiliario				
Asesores fiscales y contables externos				
Auditores externos				
Notarios				
Registradores				
Procuradores				
Actividades del Art. 2.1.ñ) Ley 10/2010 realizadas por abogados y otros profesionales				
Prestación de servicios societarios				
Transmisión de sociedades preconstituidas				
Casinos				
Loterias				
Apuestas mutuas deportivas benéficas (quinielas)				
Operaciones de juego presencial: bingos y máquinas tipo B				
Operaciones de juego presencial: apuestas deportivas				
Apuestas deportivas online				
Otros juegos online				
Consursos				
Compra-venta de joyas, piedras y metales preciosos				
Arte y antigüedades				
Comercio profesional de otros bienes de alto valor				
Inversión en bienes tangibles				
Transporte de fondos				

[35] The table contains all the information on all the sectors analysed in the 2020 NRA, not just those amended in this addendum.

9. RISKS OF NON-IMPLEMENTATION OR CIRCUMVENTION OF INTERNATIONAL FINANCIAL SANCTIONS .

The FATF Recommendations require countries to implement financial sanctions regimes to comply with United Nations Security Council (hereinafter UNSC) Resolutions relating to the prevention and suppression of terrorism and Terrorist Financing, and to the prevention, suppression and disruption of the proliferation of weapons of mass destruction and their financing (R.6, R.7, RI.10 and RI.11). Furthermore, countries must identify, assess and understand the risks of Terrorist Financing and Proliferation Financing, the latter being understood as any potential non-compliance, failure to implement or circumvention of financial sanctions relating to non-proliferation.

In line with FATF standards, this chapter analyses the risks of breaches of international financial sanctions imposed under UNSC Resolutions. It will also analyse sanctions within the framework of the European Union (EU).

9.1. Concept of international financial sanctions .

International sanctions are coercive measures that do not involve the use of armed force and which may be adopted by the UN Security Council under Chapter VII of the United Nations Charter, with the aim of influencing the actions or policies of States or other actors in the international community in order to maintain or restore international peace and security. International sanctions can take a wide variety of forms, ranging from the total or partial suspension of economic relations and communications to the severing of diplomatic relations.

Furthermore, the EU may adopt *restrictive measures* (sanctions), either on an autonomous basis or in implementation of UNSC Resolutions. These measures must be consistent with the pursuit of the objectives of the Common Foreign and Security Policy (CFSP), as set out in Article 21 of the Treaty on European Union (TEU). At EU level, therefore, there are three types of sanctions regimes, depending on the body from which they originate and their scope:

- *UN sanctions regimes*, which are transposed into EU law through the adoption of European Regulations that are binding and directly applicable in all Member States.
- *Mixed* sanctions *regimes*, in which the EU decides to reinforce UN sanctions by applying measures in addition to those imposed by the UN Security Council.
- *Autonomous* EU *regimes*, in cases where the EU itself decides to adopt restrictive measures on its own initiative.

Consequently, for the purposes of this analysis, ***international financial sanctions*** are defined as those coercive measures of a financial nature adopted by the UNSC and the EU with a view to preventing and suppressing terrorism and Terrorist Financing, and to preventing, suppressing and disrupting the proliferation of weapons of mass destruction and their financing. International financial sanctions entail an obligation on all natural or legal persons (regardless of whether they are regulated entities under Law 10/2010 of 28 April) to freeze all funds, other financial assets and economic resources owned, held or controlled, directly or indirectly, by natural or legal persons, entities, organisations or groups included on the consolidated UNSC and EU sanctions lists. They also entail a prohibition on making any funds, other financial assets or economic resources available, directly or indirectly, to sanctioned persons, or on using them for their benefit.

'Funds, other financial assets and economic resources' shall be understood to *mean* assets of any kind, whether tangible or intangible, movable or immovable, and the documents or legal instruments evidencing ownership or other rights over such assets, including bank credits, traveller's cheques, bank cheques, money orders, shares, securities, bonds, bills of exchange and letters of credit, amongst others.

'*Freezing of funds, other financial assets and economic* resources' shall be understood to mean preventing any movement, transfer, alteration, use or transaction that could result in a change in the volume, amount, location, ownership, possession, nature or destination of such funds, other financial assets and economic resources.

Failure to comply with the obligation to freeze or the prohibition on making funds, other financial assets and economic resources available to designated persons or entities constitutes an administrative offence on the part of those natural or legal persons who are obliged to do so.

9.2. International financial sanctions relating to terrorism and Terrorist Financing .

The UN Security Council has adopted a series of resolutions imposing coercive measures, including the obligation on all natural and legal persons, whether financial or non-financial, within the international community, to freeze the funds and other financial assets or economic resources of individuals and entities included in the lists approved in those resolutions:

- Due to their links with or membership of international terrorist groups (UNSC Resolutions 1267 (1999), 1988 (2011), 1989 (2011), 2253 (2015), 2610 (2021) and subsequent resolutions).
- At the request of a third country based on its own domestic lists of persons or entities linked to terrorism (UNSC Resolution 1373 (2001)).

These UNSC Resolutions have been incorporated into EU law through the following EU acts (and their subsequent amendments and updates).

In Spain, the application of international financial sanctions is regulated by Law 10/2010 of 28 April (Article 42), by its Regulation (Articles 47 and 48), and by Royal Decree 413/2015 of 29 May, which approves the Regulations of the Commission for the Supervision of Terrorist Financing Activities.

Furthermore, in accordance with current regulations, the Council of Ministers may decide to apply financial countermeasures in respect of third countries that pose higher risks of Money Laundering, Terrorist Financing or Proliferation Financing (Article 42.2 of Law 10/2010 of 28 April).

9.3. International financial sanctions relating to the proliferation of Weapons of Mass Destruction (WMD) .

The proliferation of weapons of mass destruction (WMDs), whether nuclear, chemical, radiological or biological, as well as their means of delivery, poses a serious threat to international peace and security and directly affects national security. WMD production programmes may be carried out by states, but also by non-state actors.

The capabilities of states to carry out proliferation activities or programmes differ from those of non-state actors, including their funding capabilities and the extent to which they have access to infrastructure and national entities to implement such programmes.

In the case of state actors, it should also be noted that, generally speaking, they entail the risk of similar behaviour on the part of those countries with which there is some form of confrontation or conflict, which will proceed to step up their activities relating to the production and trade of WMD. This risk of an arms race is defined as 'proliferation'.

There are several international treaties in force relating to non-proliferation to which Spain has acceded.

One of the main challenges is the control of dual-use materials, to prevent products and technology with both civilian and military uses from being employed for illicit purposes. The Treaty on the Non-Proliferation of Nuclear Weapons and the International Atomic Energy Agency's safeguards system have helped to curb and, in some cases, reverse the spread of nuclear military capability, but have not been able to prevent it entirely.

In 2004, the UN Security Council adopted Resolution 1540, which prohibits Member States from providing any form of support to non-state actors seeking to acquire, manufacture, possess, transport, transfer or use WMD and their delivery systems. The UN Security Council also extended this prohibition by identifying specific countries.

The possibility that toxic chemicals might be used against people is a particular cause for concern. Not only does the use of chemical weapons against civilians in conflict constitute a violation of international humanitarian law, but there is also a risk that terrorist groups might use chemical weapons outside conflict zones to carry out terrorist acts.

The international financial sanctions adopted by the UN Security Council aimed at preventing, suppressing and disrupting WMD are expressly linked to the activities of the Democratic People's Republic of Korea and Iran, although in the case of Iran it should be noted that on 18 October 2023 all sanctions imposed by the UNSC under Resolution 2231 (2015) were lifted.

Within the EU framework, the EU Strategy against the Proliferation of Weapons of Mass Destruction was adopted in 2003, and since then a series of (CFSP) Decisions have been adopted to update and follow up on it (in 2006, 2008, 2013 and 2017). The most recent of these is Council Decision (CFSP) 2023/654 of 20 March 2023, supporting the implementation of United Nations Security Council Resolution 1540 (2004) on the non-proliferation of weapons of mass destruction and their delivery systems. This Strategy is designed to prevent, deter, halt and, where possible, eliminate weapons of mass destruction (WMD) programmes worldwide and has the following key points:

- *Multilateralism*: Strengthening international non-proliferation mechanisms and working to improve systems for verifying breaches of the rules set out in multilateral treaties.
- *Prevention*: Fostering a stable environment at regional and international level by strengthening programmes that promote disarmament and by incorporating the objective of non-proliferation into all the EU's political, diplomatic and economic activities.
- *International cooperation*: Working closely with key partners such as the United States and NATO, and assisting third countries.

Spain has consistently highlighted the proliferation of WMD as a risk to the country's security, as set out in the National Security Strategy, which was updated in 2022. Furthermore, Russia's aggression against Ukraine has heightened the risk of Russia engaging in Proliferation Financing, as noted in the FATF's public statement.

In addition to the application of the international financial sanctions referred to above in cases of inclusion on international terrorism lists – as set out in Law 10/2010 of 28 April and in its Regulations, and which affect lists relating to the proliferation of WMDs, there is specific legislation governing foreign trade in defence and dual-use equipment, namely Royal Decree 679/2014 of 1 August, which approves the Regulations on the control of foreign trade in defence equipment, other equipment and dual-use products and technologies.

The system of penalties and sanctions is governed by two pieces of legislation:

A. The Criminal Code (Law 10/1995 of 23 November), which in Articles 566 to 568 of Chapter V 'On the possession, trafficking and storage of weapons, ammunition or explosives', classifies arms trafficking as a crime against public order, penalising conduct that constitutes a serious threat to public peace and tranquillity.
B. Law 12/1995 of 12 December on the Suppression of Smuggling, which:

- Classifies as a criminal offence (or administrative offence) the unauthorised export, import, introduction, dispatch or carrying out of any other operation subject to control, or having obtained authorisation fraudulently, of defence or dual-use material.
- Classifies as a criminal offence the commission of such acts when they involve toxic drugs, narcotics, psychotropic substances, weapons, explosives, biological agents or toxins, toxic chemicals and their precursors, or any other goods the possession of which constitutes a criminal offence, or when the smuggling is carried out through an organisation, regardless of the value of the goods, merchandise or commodities.

9.4. Vulnerabilities and sectoral risk .

Entities, particularly financial institutions, are highly aware of their obligations in this area. However, given the context of globalisation and growing financial interdependence between countries, there is always a risk of engaging in transactions subject to UNSC sanctions regimes or linked to the proliferation of WMD.

A. International financial sanctions relating to terrorism and Terrorist Financing.

In Spain, there have been no cases of individuals or entities included on EU or United Nations lists (UNSC Resolution 1267 and subsequent resolutions) being detected, nor of individuals or entities included on lists drawn up by other countries (UNSC Resolution 1373) who were clients or involved in transactions with Spanish natural or legal persons. However, taking into account the vulnerability factors arising from the volume of international transactions, their potential complexity and the high number of clients involved, it is considered that there is a moderate **inherent risk** associated with dealing with this type of client, primarily linked to entities in the financial sector with a significant international presence and operations.

Furthermore, the FATF has highlighted delays in the implementation of UNSC Resolutions caused by delays in the publication of EU Regulations, as it is these Regulations that give legal force to the UNSC Resolutions; the FATF also notes that this could lead to a greater risk of non-compliance and circumvention of financial sanctions. In order to mitigate this vulnerability arising from the timeframes, there are plans to amend the specific regulations in this area in the near future so as to bring them into line with UNSC Resolutions.

However, regulated entities, particularly those in the financial sector, are well aware of their obligations to freeze the funds and economic resources of individuals and entities listed by the UNSC and to make the necessary notifications where applicable. This awareness is particularly relevant in the credit institutions sector, which is considered to be at the highest risk with regard to international financial sanctions, owing to its greater international presence and diversity of clients; these institutions have established internal systems to carry out checks and continuously monitor the international lists issued by the UNSC.

Furthermore, the supervisory authorities carry out monitoring to verify whether financial institutions and non-financial obliged entities are complying with their legal obligations. In addition, SEPBLAC has published a *Guide to Good Practice for the Application of Lists of Persons and Entities Subject to International Financial Sanctions and Countermeasures*[36] , with the aim of providing guidance to all those obliged to comply with such duties.

[36] https://www.sepblac.es/wp-content/uploads/2018/03/aplicacion_de_listas_de_personas_y_entidades_sujetas_a_sanciones_y_contramedidas_financieras_internacionales.pdf.

B. International financial sanctions relating to the proliferation of WMD.

There are a number of risk factors in our country that must be taken into account:

- Spain's significant production of industrial equipment and technology.
- Exports of defence and dual-use equipment. In 2022, the value of defence equipment exports totalled 4,091.3 million euros, representing a 24.3 per cent increase on the previous year. 47.8% of these were to EU/NATO countries. Meanwhile, dual-use exports in 2022 were worth 289 million euros (mainly to Singapore and Norway), compared with 232 million euros the previous year[37] .
- The high volume of commercial activity, mainly via maritime traffic and national ports.
- The growing offshoring of industries linked to sensitive technologies to developing countries, which may be used to carry out indirect operations via our country.

On the other hand, it is worth noting that in the case of Spain:

- Our country is not a leading centre for international financial services.
- The Democratic People's Republic of Korea has closed its embassy in Spain.
- The Interministerial Committee on Foreign Trade in Defence and Dual-Use Materials (JIMDDU), comprising representatives from the public institutions responsible for controlling international trade in such materials, holds monthly meetings to verify and authorise imports and exports of defence and dual-use materials. Furthermore, SEPBLAC has become involved in the preparatory work of the JIMDDU, thereby strengthening the system.

These factors may imply the existence of **inherent risks** of activities aimed at concealing WMD proliferation operations involving materials produced in Spain, without there necessarily being a direct link between the entity carrying out a transaction or commercial operation and the country or the listed person/entity. It is important to bear in mind that intermediary points are not always located in high-risk jurisdictions, as countries that have traditionally been considered lower-risk are sometimes used to lend greater legitimacy to the operation and, in this way, be subject to less thorough scrutiny. Such operations may be channelled through intermediary countries by means of the triangulation of exports from Spain by so-called 'proliferators', who pose the threat in this area and are responsible for procuring the material and carrying out the commercial transaction for its shipment to the final destination.

All of this means that the inherent risk of activities related to the proliferation of WMD taking place in Spain should be considered moderate.

However, this inherent risk is reduced by the adoption of a specific national regime aimed at mitigating it, which includes regulation and authorisation procedures carried out by interdepartmental bodies that hold regular meetings and have clearly defined powers to coordinate both the authorisations and the control systems for these operations; this leads to this residual risk being classified as low/moderate.

[37] "Spanish statistics on exports of defence equipment, other equipment and dual-use products and technologies, 2022". Ministry of Industry, Trade and Tourism.

9.5. Conclusions .

A. International financial sanctions relating to terrorism and Terrorist Financing.

Although the inherent risk of financial institutions being used to circumvent the international financial sanctions established by the UN Security Council and the EU in relation to terrorism is considered to be of medium severity, the existing regulatory measures, the preventive obligations established for the sector, the administrative controls, the sector's awareness of its duties and the absence of any such cases in Spain mean that **the residual risk** is generally considered to be low. However, depending on the type and size of the institution, its transaction volume, the types of operations carried out, and the number of customers originating from or doing business with certain high-risk countries, the risk may be classified as higher. Consequently, those financial institutions with a greater presence in these countries or which conduct business with nationals or entities from these high-risk countries should be classified as moderate risk; the residual risk in the sector is therefore considered to be **low/moderate**, depending on the type of financial institution.

Meanwhile, in the **non-financial sector**, larger organisations use effective tools to detect listed individuals and entities, and although smaller organisations do not have such advanced detection systems, they are aware of their obligation to verify inclusion on the lists and act accordingly. In any case, given the nature of their activities, the level of risk is very low, with no cases having been detected in our country; the residual risk should therefore be considered **low.**

B. International financial sanctions relating to the proliferation of WMD.

The volume of commercial transactions involving defence and dual-use materials may imply the existence of vulnerabilities that could be exploited to circumvent the sanctions regime. However, although the inherent risk of financial institutions being used to circumvent the international financial sanctions established by the UNSC regarding the proliferation of WMD is considered moderate, the absence of financial and commercial relations with these countries, combined with existing regulatory measures, the obligations on the sector, administrative controls and national coordination mean that the residual risk of evading sanctions relating to the proliferation of WMD is generally considered to be **low**. However, as in the case of financial sanctions resulting from inclusion on international terrorism lists, the type of institution, its transaction volume, the types of operations carried out, the number of customers conducting business with, or having links to, those countries will influence a more detailed risk assessment. Consequently, **financial institutions** with a greater presence in these countries or conducting business with nationals or entities from these high-risk countries should be classified as moderate risk; therefore, the residual risk in the sector is considered to be **low/moderate**, depending on the type of institution.

Meanwhile, in the case of **institutions in the non-financial sector,** given the complete absence of activity with these countries, the risk should be considered **low.**

10. MEASURES TAKEN.

10.1. General measures adopted.

National Security Strategy.

The *"National Security Strategy"* adopted in 2017, which updated the previous Strategy from 2013, identified fifteen areas for action, five of which were mentioned in the 2020 NRA; the main achievements in these areas are set out below:

- Economic and financial security. Expansion of the number of countries and jurisdictions with which automatic exchange of financial information takes place , strengthening of banks' resilience and increased financial stability in the Eurozone as a result of the rules issued to reduce risks and protect deposits within the Banking Union, improved coordination of macroprudential supervision at national level[38] and the Recovery, Transformation and Resilience Plan, which sets out a roadmap for restoring economic growth, modernising the economy and creating jobs, with a view to achieving a robust, inclusive and resilient economic recovery following the COVID-19 crisis.
- The fight against organised crime. Strengthening specialised training in various aspects of the fight against terrorism and organised crime, including investigation, strategic intelligence and operational action , aimed at the LEAs, the Armed Forces, the AEAT and SEPBLAC; increasing the exchange of information on drug trafficking and organised crime; strengthening international coordination in the fight against organised crime; promoting the generation of operational and strategic intelligence produced at national level, particularly within the framework of special response plans such as that developed in the Campo de Gibraltar; in the first quarter of 2020, the annual inspection plans for drug precursors and explosives were approved; these are key to preventing the diversion of these substances towards the illicit manufacture of drugs and explosives and to verifying compliance with national and EU regulations.
- The fight against terrorism. In the area of prevention, Spain maintains its presence in various missions and is stepping up cooperation through the use of financial intelligence; in the area of protection, coordination between the different intelligence units has been strengthened and contingency plans have been drawn up; in the area of prosecution, numerous police operations continue to result in convictions and arrests.
- Cybersecurity: development of new tools aimed at strengthening capabilities; adoption of the National Guide to the Reporting and Management of Cyber Incidents; the CNI launched a plan to raise awareness, monitor and protect the computer networks of national bodies engaged in scientific research in the health and biotechnology sectors; various operations and missions carried out by the LEAs; the National Cybersecurity Forum was held, aimed at increasing public-private cooperation; the Plan to Combat Cybercrime was approved.
- Non-proliferation of weapons of mass destruction. Spain has continued to participate in the main export control regimes; coordination with EU customs authorities to prevent the illicit movement of dual-use goods and technology; collaboration with the International Association against Impunity for the Use of Chemical Weapons, which was established to increase the exchange of information on chemical weapons attacks and publicly identifies individuals and entities sanctioned for their involvement in the use of such weapons.

It should be borne in mind that, due to the impact of the COVID-19 pandemic and the increased use of hybrid strategies, a strategic review was deemed necessary to address risks and threats within a new context of globalisation, characterised by greater uncertainty and rapid change.

[38] Royal Decree 102/2019 of 1 March, establishing the Macroprudential Authority – Financial Stability Council, setting out its legal framework and elaborating on certain aspects relating to macroprudential tools.

The current 2021 National Security Strategy has a three-year timeframe. Chapter 3 lists 16 risks and threats to national security, including:

- Terrorism and violent radicalisation.
- Threats to critical infrastructure.
- Cyberspace vulnerability.
- Economic and financial instability.
- Organised crime and serious crime.
- Proliferation of weapons of mass destruction.

National Strategy against Organised Crime and Serious Crime.

One of the Strategy's priorities is the fight against human trafficking, with a specific line of action dedicated to establishing a specific national Strategic Plan against human trafficking and exploitation (PENTRA).

In accordance with the provisions of the National Strategy against Organised Crime and Serious Crime 2019–2023, efforts have continued to promote the generation of operational and strategic intelligence produced at national level, particularly within the framework of special response plans such as that implemented in the Campo de Gibraltar, or service orders and action plans concerning activities such as fraud against the tax authorities and social security, or human trafficking.

For the first time, EUROPOL has published a separate edition of the European Organised Crime Threat Assessment (SOCTA), providing a comprehensive assessment of the threats posed by financial and economic crime within the EU, with the aim, on the one hand, of highlighting the pervasiveness and destructive nature of financial and economic crime affecting neighbouring countries and, on the other, of helping all stakeholders to understand the wide variety of financial and economic crimes. Specifically, the report analyses all financial and economic crimes affecting the EU, such as Money Laundering, corruption, fraud, intellectual property offences, and the counterfeiting of goods and currency.

National Counter-Terrorism Strategy.

The Specialised Committee on Counter-Terrorism (CECT) established Working Group I for the Monitoring and Evaluation of the National Counter-Terrorism Strategy (ENCOT), which, in its 2020 ENCOT Evaluation Report (IEE), identified 30 priority measures to combat terrorism.

During the period 2020–2023, various actions have been carried out, many of which fall within the framework of the National Strategic Plan against Terrorist Financing (PENCFIT) and the National Strategic Plan for the Prevention and Combating of Violent Radicalisation (PENCRAV). These plans were approved by the National Security Council at its meeting on 6 October 2020.

Section 4.6 details some of the achievements of the PENCFIT and the PENCRAV.

10.2. Other specific mitigation measures.

Extension of the scope of regulated entities: virtual asset service providers and others.

Royal Law 7/ 2021 of 27 April established that any persons carrying out activities involving the exchange of virtual currency for fiat currency and the custody of electronic wallets must be registered in a register maintained by the Banco de España . This regulatory amendment, which affected Law 10/2010 of 28 April, enabled providers of services

involving the exchange of virtual currency for fiat currency and the custody of electronic wallets to be included as regulated entities.

This regulatory adaptation helped bring our preventive legislation into line with FATF international standards and to incorporate the provisions of EU Directive 2018/843 regarding the inclusion of providers of services involving the exchange of virtual currency for legal tender or between different virtual currencies, and those offering electronic wallet custody services, into Law 10/2010, of 28 April.

Furthermore, a second additional provision was introduced, requiring CASP to register with a special register at the Banco de España. To obtain registration, these entities must demonstrate that they have adequate procedures and bodies in place for the prevention of Money Laundering and terrorist financing. The existence of such procedures is reviewed by the Commission's Executive Service, which must issue a report on the matter for inclusion in the administrative registration file maintained by the Banco de España.

Royal Decree 7/2021 of 27 April lists the following as regulated entities:

- Authorised insurance undertakings that deal with investments and not solely in the life insurance sector.
- Electronic money institutions and payment institutions, to which are added the natural and legal persons referred to in Articles 14 and 15 of Royal Decree-Law 19/2018 of 23 November.
- Persons who carry out, on a professional basis, any activity provided for in Article 6.1 of Law 5/2015 of 27 April, or who carry out lending activities provided for in Law 5/2019 of 15 March.
- Those who are professionally engaged in the letting of immovable property involving a transaction with a total annual rent of 120,000 euros or more, or a monthly rent of 10,000 euros or more.
- Auditors, external accountants, tax advisers and any other person who undertakes to provide, either directly or through related parties, material assistance, support or advice on tax matters as their main business or professional activity.
- This also includes intermediaries in the trade in works of art or antiques, as well as persons who store or trade in works of art or antiques or act as intermediaries in the trade in works of art or antiques when carrying out such activities in free ports.

Strengthening of cross-border control systems for the movement of cash and means of payment.

Commission Implementing Regulation (EU) 2021/776 of 11 May 2021 established the templates for certain forms, as well as the technical standards for the effective exchange of information pursuant to Regulation (EU) 2018/1672 of the European Parliament and of the Council on controls on the entry into or exit from the Union of cash. This Regulation was supplemented by Order ETD/1217/2022 of 29 November, which regulates declarations of movements of means of payment in the context of the prevention of Money Laundering and terrorist financing.

In Spain, there is an obligation to declare intra-Community movements of means of payment exceeding 10,000 euros and movements within the national territory above a threshold of 100,000 euros. In this regard, the **forms for** declaring movements of means of payment were amended to expand and clarify the information relating to these movements.

The regulatory amendment of 2022 affected the regime for declaring movements of means of payment established in Article 34 of Law 10/2010 of 28 April. The most significant changes were as follows:

- The obligation to declare upon entry into and exit from Spanish territory, imposed on individuals travelling with means of payment amounting to 10,000 euros or more, was extended to cover movements of means of payment carried out without being accompanied by an individual, such as postal consignments, courier deliveries, unaccompanied luggage or containerised cargo.

- It was further stipulated that, for the purposes of the Law, commodities used as highly liquid stores of value, such as gold, are considered means of payment.

Creation of the Central Register of Beneficial Ownership and interconnection with EU registers, along with greater transparency and information on service providers to companies and trust-type trusts.

The Central Register of Beneficial Ownership (RCTIR) was launched on 19 September 2023. It is a single central register covering the whole of the national territory, managed by the Ministry of the Presidency, Justice and Relations with Parliament, and is based at the Directorate-General for Legal Security and Public Trust, which is the body in charge of its management and responsible for it.

The purpose of the RCTIR is to collect and publish information on current beneficial ownership relating to all Spanish legal persons, trusts and similar entities or structures without legal personality operating in Spain. The RCTIR holds historical data on Spanish legal entities, trust-type trusts and similar entities or structures without legal personality operating in Spain, which will be accessible to the authorities. The aim is to achieve greater transparency in the use of companies and other legal entities, trust-type trusts and similar legal instruments, thereby safeguarding the integrity of the financial system.

The RCTIR will obtain its information regarding Spanish legal entities from official sources, such as the Spanish Association of Registrars of Property, Commercial and Movable Assets (via the Commercial Registers) or the General Council of Notaries, and will also include the register of trust-type trusts and other legal instruments analogous to trusts operating in Spain through direct declaration by the trustee, enabling the beneficial ownership of all such entities to be checked.

Changes to enquiries and reportable assets in the Financial Ownership Register.

Organic Law 9/2022 of 28 July, laying down rules to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of criminal offences, transposes Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 and regulates access to the FTF.

Its aim is to improve the prosecution of financial crimes, combat Money Laundering and terrorist financing, and prevent tax offences. The regulatory amendment seeks to facilitate the exchange of information in the fight against Money Laundering and terrorist financing, and grants access to the FTF to authorities conducting investigations aimed at the prevention, detection, investigation and prosecution of serious criminal offences.

Furthermore, it is worth noting the removal of the requirement for prior judicial authorisation or authorisation from the Public Prosecutor's Office for LEAs to access the FTF. The information shared contains the identifying details of account holders, but does not include information on balances or transactions. In other words, access is permitted to the identification of the financial product, the credit institution' , and the account or product holders and authorised users. However, should access beyond this data be required, prior authorisation from a court or the Public Prosecutor's Office will be necessary.

Furthermore, other amendments were introduced to expand the information contained in the FTF. Specifically, the first final provision of Organic Law 9/2022 of 28 July amended Article 43 of Law 10/2010 of 28 April on the prevention of Money Laundering and terrorist financing, introducing, amongst other things, the following changes:

- The obligation to report to the FTF, which until then had been limited to credit institutions, was extended to payment institutions and electronic money institutions.

- The list of product types for which reporting to the Financial Ownership Register is mandatory was also extended, adding to that list any type of payment account and safe-deposit box rental contracts.
- As regards the content of the declarations, it became mandatory to declare the beneficial owners of the products.

Increased national cooperation.

Law 18/2022 of 28 September, through its Second Additional Provision, amended Law 10/2010 of 28 April on the prevention of Money Laundering and terrorist financing.

Among the new provisions introduced by this amendment, there are two that promote risk mitigation:

- The addition of Article 32 ter, which enables obliged entities belonging to the same category as those set out in Article 2 of the Law to establish common systems for the collection, storage and, where appropriate, access to the information and documentation gathered for the purpose of complying with due diligence obligations.
- The addition of Article 33, relating to centralised fraud prevention databases, for the exchange of information between obliged entities.

In addition, the supervisory agreements with the prudential supervisors (Banco de España, CNMV and the Directorate-General for Insurance and Pension Funds) have been renewed, strengthening existing cooperation in the area of Money Laundering/CFT supervision.

Change to the system for assessing reports based on indications.

Among the functions of the Commission's Executive Service is the assessment of the quality of reports received from regulated entities. Changes have recently been made to the assessment system, with new elements introduced to improve these assessments, such as the 'relevance' factor, which quantifies various factors: the seriousness of any potential criminal activities underlying the reported transactions, the total value of the reported transactions, the depth of the comprehensive analysis, and the novelty of the reported patterns.

Supervisory measures.

Alongside the investigations carried out by the LEAs, the supervision of regulated entities is one of the main measures adopted by the authorities to mitigate risks. In recent years, SEPBLAC, in its capacity as a supervisory authority, has carried out specific inspections targeting regulated entities in specific sectors which, due to their characteristics, present Money Laundering/Terrorism Financing risks. These include sector-specific and thematic inspections, requests for structured information from regulated entities, and consideration of the risk factors identified in the 2020 NRA to assess the risks posed by regulated entities.

Measures relating to financial sanctions.

Since the approval of the 2020 National Risk Analysis, a series of measures have been implemented with the aim of improving the enforcement of international financial sanctions.

At an operational level, the Sanctions Enforcement Monitoring Working Group and the Ad Hoc Group on Frozen and Seized Assets have been established. Both groups comprise representatives from departments with responsibilities

for the implementation of international sanctions. The first group is more strategic in nature, comprising representatives from the relevant directorates, and focuses on coordinating the activities of all these departments within their respective fields. The Ad Hoc Group on Frozen and Seized Assets, on the other hand, is much more operational in nature, dedicated to the exchange of information, the detection and freezing of assets.

With regard to dissemination and awareness-raising, the Sub-Directorate-General for the Inspection and Control of Capital Movements has set up the institutional email addresssancionesfinancieras@economia.gob.es as a general enquiry channel for both the public and private sectors. This has made it possible to broaden the reach of all updates and developments regarding international sanctions, as well as to clarify technical queries and doubts concerning their implementation. Consequently, the number of enquiries received regarding international financial sanctions has risen from 4 in 2021 to 220 in 2022.

In addition, all documentation available on the website of the Directorate-General for the Treasury and Financial Policy relating to this subject has been updated. This includes new guides and guidance on the implementation of international financial sanctions, a new document for requesting the unfreezing of funds, links to frequently asked questions answered by the European Commission, and a new *whistleblowing* channel.

11. CONCLUSIONS.

Since the adoption of the previous NRA, the Spanish anti-money laundering system has faced new developments and changes, both external and internal, which **made it necessary to update the risks identified in 2020.**

Among these developments, we can highlight the transposition of the Fifth Directive on the prevention of the use of the financial system for the purposes of Money Laundering or Terrorist Financing into Spanish AML/CFT legislation, which has strengthened the Spanish preventive system through measures such as the inclusion of new obliged entities, the strengthening of the system for identifying the beneficial owners of legal entities, the amendment of the assets subject to reporting, and the expansion of the number of reporting entities.

Similarly, the COVID-19 pandemic presented new challenges for the Spanish preventive system, particularly in relation to criminal activities that exploited the vulnerabilities arising from the accelerated need for the digitalisation of the Spanish economy and society.

Furthermore, the risk associated with cross-border activity in Europe has increased as a result of the war between Russia and Ukraine, particularly in relation to cash movements by migrant populations, the diversion of weapons used in the conflict for criminal purposes, the trade in defence and dual-use equipment, and the use of clandestine channels for money flows to evade sanctions.

The Money Laundering **threats** identified in Spain as a result of national cooperation between authorities are in line with those set out in the previous version of the NRA: organised crime, drug trafficking, and economic and financial crimes associated with fraud and corruption. Although the number of organised crime groups operating in Spain has fallen, the interconnection between different international organisations has grown, as has the combination of various underlying offences associated with fraud, drug trafficking or human trafficking.

Fraud involving digital operations currently poses the greatest threat, with the use of so-called 'money mules' and the creation of 'mule' accounts to move funds making it difficult to trace the money and identify the actual offender.

As for drug trafficking, although the most prevalent substances are hashish and cocaine, there is concern over Spain's position as the leading producer of cannabis in the EU, as well as warnings regarding the circulation and consumption amongst the Spanish population of a range of drugs not covered by international control conventions, known *as New Synthetic Substances*.

Furthermore, jihadist terrorism continues to be the most significant global threat. It is a fact that funding is channelled through small cells or radical individuals who make use of the fragmentation of funds and crypto-assets, which hinder transparency and traceability.

The **vulnerabilities** identified in Spain that exacerbate the risks associated with these threats include factors relating to the population and the number of immigrants; geographical factors arising from the identification of areas within the country with greater exposure to Money Laundering risks; the high use of cash; and the increasing presence of technological innovations in the Spanish economy.

With regard to the **sectors assessed** in this update, it is worth noting that, although there has been no change in their residual risks – with the exception of the execution of payment transactions (other payment institution services) – certain circumstances, such as regulatory changes, supervisory actions or alterations to specific characteristics, have prompted an analysis of the risks affecting them.

Finally, an assessment has been carried out of the mitigation measures proposed in the previous NRA that have been adopted to date. Generally speaking, objectives relating to the fight against organised crime, the ' ' cybersecurity, non-proliferation and the fight against terrorism have been achieved. On this last point, the actions carried out within the framework of the ENCOT and its strategic plans (PENCFIT and PENCRAV) are particularly relevant. More specifically,

the measures implemented following the transposition of the Fifth Directive into national law (creation of the Register of Beneficial Ownership, inclusion of obliged entities, etc.) are of particular importance, as is the increased monitoring of declarations of cross-border fund movements and the supervisory actions carried out.

Despite these achievements, it must be borne in mind that, at present, the Spanish preventive system is constantly facing new challenges arising from newly detected operations, new actors involved, or identified needs. Consequently, ongoing monitoring of the implementation of the actions set out within the national strategies that form the general mitigating measures is crucial. More specifically, measures have been put in place to address shortcomings observed in the legislative, supervisory, investigative and judicial prosecution spheres.

12. STATISTICS.

See the publication of the Statistical Information Report 2018–2022 and its Annex.

https://www.tesoro.es/prevencion-del-blanqueo-y-movimiento-de-efectivo/comision-de-prevencion-del-Money Laundering-e-infracciones-monetarias/estadisticas-e-informes/estadisticas

Abbreviations used

AEAT. State Tax Administration Agency.

AEB. Spanish Banking Association.

AEF. Spanish Association of Foundations.

AECID. Spanish Agency for International Development Cooperation.

AEJPR. Spanish Association of Jewellers, Silversmiths and Watchmakers,

AENPA. Spanish Association of Payment Institutions.

ASNEF. National Association of Credit Institutions.

Money Laundering.

AML/CFT. Money Laundering and Terrorist Financing.

CA. Crypto-assets.

CASP. Crypto-asset service providers

CECA. Spanish Confederation of Savings Banks.

CECT. Specialised Committee on Counter-Terrorism.

CGI. General Information Directorate. Policía Nacional.

CGPJ. General Council of the Judiciary.

CII. Collective Investment Institutions.

CITCO. Centre for Intelligence against Terrorism and Organised Crime.

CNI. National Intelligence Centre.

CNMV. National Securities Market Commission.

CRAB. Anti-Money Laundering Registry Centre.

DGSFP. Directorate-General for Insurance and Pension Funds.

ECB. European Central Bank.

FAF. Financial Advisory Firms.

EBA. European Banking Authority.

EMI. Electronic Money Institutions.

EFC. Credit Institutions.

ENCOyDG. National Strategy against Organised Crime and Serious Crime.

ENCOT. National Strategy against Terrorism.

FGE. Prosecutor General's Office.

FT. Terrorist Financing.

FTF. Financial Ownership Register.

FATF. Financial Action Task Force.

GOIF. Financial Intelligence Task Force.

GRUSEFIT. Working Group III for the Monitoring and Implementation of the National Strategic Plan to Combat Terrorist Financing

ICAC. Institute of Accounting and Auditing.

ICO. Initial Coin Offering. Initial offering of coins (crypto-assets).

JI. Guardia Civil Information Directorate.

NGDOs. Non-Governmental Development Organisations.

NRA. National Risk Assessment.

NPO. Non-profit organisations.

OCP. Centralised Prevention Body.

PFP. Crowdfunding Platforms.

PELCEIL – Strategic Plan to Combat the Illicit Enrichment of Criminal Organisations and Offenders.

PENCFIT. National Strategic Plan to Combat Terrorist Financing.

PENCRAV. National Strategic Plan to Prevent and Combat Violent Radicalisation.

PEP-PRP. Persons in Public Responsibility.

P-N CGPJ. General Directorate of the Judicial Police. Policía NacionaL

RECTIR. Register of Beneficial Ownership.

SAREB. Asset Management Company for Assets Arising from Bank Restructuring.

SEPBLAC. Executive Service for the Prevention of Money Laundering.

MGS. Mutual Guarantee Societies.

SGIIC. Collective Investment Scheme Management Companies.

SICAV. Open-Ended Investment Companies.

SNCE. National Electronic Clearing System.

SNRA. (EU) Supra-National Risk Analysis.

SOCIMI. Listed Real Estate Investment Companies.

SVA. Customs Surveillance Service.

UCO. Central Operational Unit of the Guardia Civil.

UDEF. Central Unit for Economic and Fiscal Crime. Policía Nacional.

FIU. Financial Intelligence Unit.

UNACC. National Union of Credit Cooperatives.

UNODC. United Nations Office on Drugs and Crime.

UNSCR. United Nations Security Council Resolutions.

UTPJ. Criminal Intelligence Unit of the Guardia Civil.

List of key regulatory provisions

- Law 19/2003 of 4 July on the legal framework governing capital movements and economic transactions with foreign countries.
- Law 4/2010 of 10 March on the enforcement within the EU of judicial confiscation orders.
- Law 10/2010 of 28 April on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT).
- Law 31/2010 of 27 July on the simplification of the exchange of information and intelligence between the security services of EU Member States.
- Law 13/2011 of 27 May on the regulation of gambling.
- Royal Decree-Law 11/2018 of 31 August transposing directives on the protection of pension commitments to employees, the prevention of Money Laundering, and entry and residence requirements for third-country nationals.
- Royal Decree-Law 7/2021 of 27 April transposing European Union directives on competition, Money Laundering, credit institutions, telecommunications, tax measures, the prevention and remediation of environmental damage, the posting of workers in the provision of cross-border services, and consumer protection.
- Law 18/2022 of 28 September on the creation and growth of businesses.
- Law 2/2023 of 20 February regulating the protection of persons reporting regulatory infringements and combating corruption.
- Royal Decree-Law 5/2023 of 28 June, adopting and extending certain measures in response to the economic and social consequences of the war in Ukraine, in support of the reconstruction of the island of La Palma and other situations of vulnerability; transposing European Union Directives on structural changes to commercial companies and the work-life balance for parents and carers; and on the implementation and enforcement of European Union law.
- Royal Decree 304/2014 of 5 May, approving the Regulations under Law 10/2010 of 28 April for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT).
- Royal Decree 413/2015 of 29 May, approving the Regulations of the Commission for the Supervision of Terrorist Financing Activities.
- Royal Decree 948/2015 of 23 October regulates the Office for Asset Recovery and Management.
- Royal Decree 609/2023 of 11 July, establishing the Central Register of Beneficial Ownership and approving its Regulations.
- Order ECO/2652/2002 of 24 October and Order EHA/1464/2010 of 28 May, implementing the obligations to report transactions relating to certain countries to the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences.
- Order EHA/2963/2005, of 20 September, regulating the Centralised Body for the Prevention of Money Laundering within the General Council of Notaries.
- Order EHA/1439/2006, of 3 May, regulating the reporting of movements of means of payment in the context of the prevention of Money Laundering.
- Order EHA/2619/2006, of 28 July, implementing certain Money Laundering obligations for regulated entities engaged in currency exchange or the management of international transfers.
- Order EHA/2444/2007, of 31 July, concerning the external expert's report on the internal control and reporting procedures and bodies established to prevent Money Laundering.
- Order EHA/114/2008, of 29 January, regulating compliance with certain obligations of notaries in the field of Money Laundering prevention.
- Order ECC/2503/2014, of 29 December, establishing the personal data register known as the 'Financial Ownership Register' (FTF).

- Order ECC/2402/2015, of 11 November, establishing the Centralised Body for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) within the Association of Registrars of Property, Commercial and Movable Assets.
- Order ETD/1217/2022 of 29 November, regulating declarations of movements of means of payment in the context of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT).