

v

Fargo S.p.A. AML. CFT. Policy 2026

DOCUMENT CLASSIFICATION NOTICE

All documents issued by **Fargo S.p.A.** are classified in accordance with the Company's internal information classification framework, as set out below:

PUBLIC

documents are intended for unrestricted distribution and may be disclosed to any third party without limitation.

COMPANY CONFIDENTIAL

documents are intended solely for internal use within Fargo S.p.A. and may be shared only with authorised personnel or external parties where strictly necessary for business or regulatory purposes and subject to appropriate confidentiality obligations.

HIGHLY CONFIDENTIAL

documents contain sensitive commercial, operational, legal, or compliance-related information and are restricted to specifically authorised individuals within Fargo S.p.A. Access, disclosure, or distribution of such documents is strictly limited and controlled.

All documents must be handled, stored, and distributed in accordance with their assigned classification and applicable confidentiality and data protection requirements.

FARGO S.p.A



INDEX

(TABLE OF CONTENTS)

DOCUMENT CONTROL AND GOVERNANCE

Document Classification Notice
Document Control Information
Document Ownership and Approval
Document Distribution List
Policy Version Control Record – Revision History
Policy Approval and Acknowledgement
Definitions and Interpretation

ANTI-MONEY LAUNDERING (AML) AND COUNTER-TERRORIST FINANCING (CFT) POLICY

- 1. Policy Statement**
- 2. Confidentiality and Use of the Policy**
- 3. Legal and Regulatory Framework**
 - 3.1 Italian Legislative Framework
 - 3.2 European Union Framework
 - 3.3 International Standards
- 4. Objectives of the Policy**
 - 4.1 Prevention of Money Laundering and Terrorist Financing
 - 4.2 Adoption of a Documented Risk-Based Approach
 - 4.3 Regulatory Compliance
 - 4.4 Governance, Accountability, and Escalation
 - 4.5 Detection and Reporting of Suspicious Activity
 - 4.6 Protection of the Company's Integrity and Continuity
- 5. Scope of Application**
 - 5.1 Business Activities and Transactions
 - 5.2 Customers, Counterparties, and Business Relationships
 - 5.3 Directors, Employees, and Relevant Third Parties
 - 5.4 Lifecycle of the Customer Relationship
 - 5.5 Contractual and Professional Obligations
 - 5.6 Cash Transactions Policy
- 6. Governance and Three Lines of Defence**
 - 6.1 First Line of Defence – Operational Functions
 - 6.2 Second Line of Defence – Compliance Function

6.3 Third Line of Defence – Independent Review and Audit

6.4 Role of the Board of Directors

6.5 Escalation and Reporting Lines

7. Definitions and Interpretation

8. Roles and Responsibilities

8.1 Board of Directors

8.2 Senior Management

8.3 Responsabile Antiriciclaggio (AML Compliance Officer)

8.4 Employees and Relevant Third Parties

9. Money Laundering and Terrorist Financing Risk-Based Approach

9.1 Principles of the Risk-Based Approach

9.2 Risk Factors Considered

9.3 Timing of Risk Assessments

9.4 Risk Classification and Mitigation

9.5 Documentation and Governance

10. Customer Due Diligence (CDD)

10.1 General Principles

10.2 Circumstances Requiring CDD

10.3 Identification and Verification of Natural Persons

10.4 Identification and Verification of Legal Persons

10.5 Beneficial Ownership Identification

10.6 Purpose and Intended Nature of the Relationship

10.7 Ongoing Due Diligence and Monitoring

10.8 Refusal, Suspension, and Termination

11. Enhanced Due Diligence (EDD)

11.1 Purpose and Regulatory Basis

11.2 Circumstances Requiring EDD

11.3 Enhanced Due Diligence Measures

11.4 Senior Management Approval

11.5 Ongoing Enhanced Monitoring

11.6 Failure to Satisfy EDD Requirements

12. Politically Exposed Persons (PEPs)

12.1 Regulatory Definition and Scope

12.2 Domestic, Foreign, and International Organisation PEPs

12.3 Identification and Screening

12.4 Due Diligence Measures for PEPs

12.5 Cooling-Off Period and Risk Downgrading

12.6 Refusal, Suspension, and Termination

13. Sanctions and Restrictive Measures

- 13.1 Applicable Sanctions Framework
- 13.2 Sanctions Risk Exposure
- 13.3 Sanctions Screening Procedures
- 13.4 Handling of Potential Matches and False Positives
- 13.5 Confirmed Sanctions Matches
- 13.6 Record-Keeping and Audit Trail
- 13.7 Training and Awareness

14. Suspicious Transaction Reporting (SOS)

- 14.1 Legal Obligation to Report
- 14.2 Internal Identification of Suspicious Activity
- 14.3 Internal Escalation Procedures
- 14.4 Assessment by the Compliance Function
- 14.5 Decision to Submit an SOS
- 14.6 Timing and Transaction Suspension
- 14.7 Confidentiality and Prohibition of Tipping-Off
- 14.8 Documentation and Record-Keeping

15. Record-Keeping and Data Retention

- 15.1 Regulatory Basis and Objectives
- 15.2 Categories of Records Maintained
- 15.3 Retention Periods
- 15.4 Storage, Security, and Access Control
- 15.5 Data Protection and Confidentiality
- 15.6 Audit Trail and Traceability
- 15.7 Availability to Authorities and Auditors

16. Training and Awareness

- 16.1 Training Objectives
- 16.2 Scope and Target Audience
- 16.3 Training Content
- 16.4 Frequency and Delivery Methods
- 16.5 Board and Senior Management Training
- 16.6 Documentation and Evidence of Training
- 16.7 Assessment of Training Effectiveness
- 16.8 Awareness and Ongoing Communication

17. Independent Review, Audit, and Remediation

- 17.1 Independent Review Framework
- 17.2 Scope and Methodology of Audits
- 17.3 Reporting of Findings
- 17.4 Remediation and Corrective Actions

- 17.5 Tracking and Follow-Up
- 17.6 Continuous Improvement

18. Policy Review, Governance Cycle, and Continuous Improvement

- 18.1 Policy Review Cycle
- 18.2 Governance and Change Management
- 18.3 Communication and Implementation of Updates
- 18.4 Continuous Improvement

19. Entry into Force and Board Approval

- 19.1 Entry into Force
- 19.2 Board Approval and Accountability
- 19.3 Implementation and Oversight
- 19.4 Formal Approval Record

ANNEXES

Annex A – AML/CFT Risk Assessment Methodology

Annex B – Customer Risk Classification Matrix

Annex C – Customer Due Diligence (CDD) & Enhanced Due Diligence (EDD)
Documentation Requirements

Annex D – Suspicious Activity Indicators and Typologies

Annex E – Record Retention Schedule and Access Controls

**ANTI-MONEY LAUNDERING (AML)
& COUNTER-TERRORIST FINANCING (CFT)
POLICY AND PROCEDURE**

DOCUMENT CONTROL INFORMATION

Title	Anti-Money Laundering (AML) & Counter-Terrorist Financing (CFT) Policy and Procedure
Department	Compliance Function
Information Classification	Company Confidential
Policy Applicable To	Fargo S.p.A.
Registered Address	Via Monte Sabotino, 2 – 24121 Bergamo (BG), Italy
Company Registration	C.F./P. IVA 09019870964
Current Version	1.5
Effective Date	_____
Review Cycle	Annually
Next Scheduled Review	_____

DOCUMENT OWNERSHIP AND APPROVAL

Role	Designation
Author / Owner	Responsabile Antiriciclaggio (AML Compliance Officer)
Reviewed By	Senior Management / Compliance Function
Approved By	Board of Directors – Fargo S.p.A.

DOCUMENT DISTRIBUTION LIST

S. No. Distribution

- 1 Board of Directors
- 2 Senior Management
- 3 All Employees of Fargo S.p.A.
- 4 Compliance Function
- 5 External Auditors (upon request)
- 6 Banking Partners (upon request)

POLICY VERSION CONTROL RECORD – REVISION HISTORY

Version	Policy Name	Reason for Implementation / Revision	Effective Date	Next Review Date
1.0	AML & CFT Policy and Procedure	Initial adoption in accordance with Italian and EU AML law	_____	_____

POLICY APPROVAL AND ACKNOWLEDGEMENT

The undersigned confirm that they have reviewed and approved this Anti–Money Laundering (AML) & Counter–Terrorist Financing (CFT) Policy and Procedure of Fargo S.p.A. and acknowledge responsibility for ensuring its effective implementation.

Any amendments to this Policy shall be made only upon recommendation by the Compliance Function and formal approval by the Board of Directors.

Name and Title	Signature	Date
Board Representative	_____	_____
AML Compliance Officer	_____	_____

DEFINITIONS AND INTERPRETATION

(For the purposes of this Policy)

AML Compliance Officer (Responsabile Antiriciclaggio)

The person appointed pursuant to Legislative Decree 231/2007 responsible for oversight, implementation, and reporting of AML/CFT obligations.

Money Laundering (Riciclaggio)

Any act intended to conceal or disguise the illicit origin of proceeds derived from criminal activity, including:

- Conversion or transfer of assets
- Concealment or disguise of the nature, source, location, or ownership of assets
- Acquisition, possession, or use of proceeds of crime.

(Articles 648-bis and 648-ter.1 Italian Criminal Code)

Terrorist Financing (Finanziamento del Terrorismo)

The provision or collection of funds, directly or indirectly, with the intention or knowledge that they be used to carry out terrorist acts, regardless of the origin of the funds.

Politically Exposed Persons (PEP)

Natural persons who are or have been entrusted with prominent public functions, including domestic, foreign, and international PEPs, as well as their family members and close associates, as defined under Legislative Decree 231/2007.

High-Risk Customer

A customer presenting elevated AML/CFT risk due to:

- Geographic exposure
- Complex ownership structures

- PEP involvement
- Cash-intensive activities
- Unusual transaction patterns.

Sanctions and Restrictive Measures

Measures adopted by:

- The European Union
- The United Nations
- Italian authorities

including asset freezes, prohibitions on funds or economic resources, and trade restrictions.

Funds

Assets of any kind, tangible or intangible, movable or immovable, including:

- Currency
- Financial instruments
- Digital or electronic assets
- Rights or claims to such assets.

Proceeds

Funds generated directly or indirectly from criminal activity, including profits, economic benefits, or converted assets.

Source of Funds (SoF)

The origin of funds used in a specific transaction or relationship.

Source of Wealth (SoW)

How a customer's overall wealth or net worth was accumulated.

Suspicious Transaction (Operazione Sospetta)

Any transaction or attempted transaction for which there are reasonable grounds to suspect money laundering or terrorist financing.

Suspicious Transaction Report (SOS)

A report submitted to the Unità di Informazione Finanziaria (UIF) pursuant to Articles 35–41 of Legislative Decree 231/2007.

Risk-Based Approach (RBA)

A methodology whereby AML/CFT controls are applied proportionately to the level of risk identified.

Targeted Financial Sanctions

Sanctions imposed under EU or UN frameworks relating to terrorism or proliferation financing.

ANTI-MONEY LAUNDERING (AML) AND COUNTER-TERRORIST FINANCING (CFT) POLICY

Fargo S.p.A.

Via Monte Sabotino, 2 – 24121 Bergamo (BG), Italy

C.F. / P. IVA: 09019870964

1. POLICY STATEMENT

Fargo S.p.A. (the “**Company**”) adopts this Anti-Money Laundering and Counter-Terrorist Financing Policy (the “**Policy**”) to formally set out the principles, governance framework, internal controls, and operational procedures implemented to prevent, detect, and mitigate the risks of money laundering, terrorist financing, and related financial crimes.

The Company operates in the precious metals and gold sector, a business area recognised at both European and international level as inherently exposed to elevated AML/CFT risk. For this reason, Fargo S.p.A. applies a conservative, risk-based, and fully documented compliance approach aligned with Italian law, European Union legislation, and international standards.

This Policy reflects the Company’s commitment to:

- Acting with integrity and transparency
- Protecting the financial system from abuse
- Cooperating fully with competent authorities
- Maintaining the confidence of banking partners, auditors, regulators, and counterparties.

Compliance with this Policy is mandatory for all directors, officers, employees, consultants, and any third party acting on behalf of Fargo S.p.A.

2. CONFIDENTIALITY AND USE OF THE POLICY

This Policy, together with all related procedures, risk assessments, and annexes, constitutes confidential internal documentation of Fargo S.p.A.

It may be disclosed exclusively to:

- Italian or European supervisory authorities
- Financial institutions for due-diligence purposes
- External auditors and professional advisers

- Law enforcement or judicial authorities where required by law.

Unauthorised disclosure, reproduction, or use for purposes other than compliance and regulatory review is strictly prohibited.

3. LEGAL AND REGULATORY FRAMEWORK

3.1 Italian Legislative Framework

This Policy is adopted in accordance with **Legislative Decree No. 231 of 21 November 2007**, as amended (the Italian AML Act), which transposes European AML Directives into Italian law and governs the prevention of money laundering and terrorist financing.

In particular, the Policy reflects the obligations set out under:

- Articles 15–23 (Risk-Based Approach and Customer Due Diligence);
- Articles 24–25 (Enhanced Due Diligence);
- Articles 31–34 (Record-keeping);
- Articles 35–41 (Suspicious Transaction Reporting);
- Relevant implementing regulations and guidance issued by the **Unità di Informazione Finanziaria per l'Italia (UIF)** at the **Banca d'Italia**.

3.2 European Union Framework

The Policy further implements the requirements of:

- Directive (EU) 2015/849 (4th AML Directive);
- Directive (EU) 2018/843 (5th AML Directive);
- Directive (EU) 2018/1673 (6th AML Directive);
- Regulation (EU) 2015/847 on information accompanying transfers of funds;
- Guidelines issued by the European Banking Authority (EBA) and other European Supervisory Authorities, where applicable.

3.3 International Standards

Fargo S.p.A. aligns its AML/CFT framework with the **Financial Action Task Force (FATF)** Recommendations, insofar as they are incorporated into EU and Italian law and recognised supervisory practice.

4. OBJECTIVES OF THE POLICY

The objectives of this Policy are to establish a comprehensive, coherent, and enforceable AML/CFT framework proportionate to the nature, scale, and complexity of the activities carried out by Fargo S.p.A., and consistent with applicable Italian and European regulatory expectations.

In particular, this Policy aims to:

4.1 Prevention of Money Laundering and Terrorist Financing

Prevent Fargo S.p.A. from being used, intentionally or unintentionally, as a vehicle for money laundering, terrorist financing, or related financial crimes. This objective is achieved through the implementation of robust preventive controls, including customer due diligence, transaction monitoring, sanctions screening, and suspicious transaction reporting mechanisms designed to identify and mitigate illicit activity at the earliest possible stage.

4.2 Adoption of a Documented Risk-Based Approach

Establish and maintain a documented, structured, and proportionate Risk-Based Approach (RBA) that enables Fargo S.p.A. to identify, assess, understand, and manage money laundering and terrorist financing risks associated with its customers, products, services, transactions, and geographic exposure. The RBA ensures that enhanced controls are applied where higher risks are identified, while lower-risk activities are managed in a proportionate and efficient manner.

4.3 Regulatory Compliance

Ensure full and ongoing compliance with all applicable Italian and European Union AML/CFT legal and regulatory obligations, including Legislative Decree 231/2007, EU AML Directives, directly applicable EU Regulations, and guidance issued by competent authorities. This includes the timely implementation of legislative changes and supervisory expectations into internal policies and procedures.

4.4 Governance, Accountability, and Escalation

Define clear governance arrangements, roles, responsibilities, and escalation mechanisms across all levels of the organisation. This objective ensures that AML/CFT responsibilities are clearly allocated, decision-making authority is appropriately defined, and potential issues are escalated promptly to the Compliance Function, senior management, and the Board of Directors, as appropriate.

4.5 Detection and Reporting of Suspicious Activity

Enable the timely identification, assessment, and reporting of suspicious transactions or behaviours to the competent authorities, in particular the Unità di Informazione

Finanziaria (UIF). This includes ensuring that staff are adequately trained to recognise indicators of suspicious activity and that internal reporting and decision-making processes operate independently, objectively, and without undue delay.

4.6 Protection of the Company's Integrity and Continuity

Preserve the reputation, operational continuity, and financial integrity of Fargo S.p.A. by mitigating legal, regulatory, financial, and reputational risks arising from money laundering or terrorist financing exposure. This objective supports the Company's long-term sustainability, banking relationships, and stakeholder confidence.

5. SCOPE OF APPLICATION

This Anti-Money Laundering and Counter-Terrorist Financing Policy applies comprehensively across **all activities, functions, and organisational levels** of Fargo S.p.A., without exception.

5.1 Business Activities and Transactions

This Policy applies to **all business activities and transactions** carried out by Fargo S.p.A., whether conducted on a one-off or ongoing basis. This includes, but is not limited to, activities relating to the purchase, sale, handling, storage, and transfer of precious metals, as well as any ancillary or supporting activities connected to such operations.

The Policy applies irrespective of:

- Transaction size or frequency
- Method of execution
- Whether the transaction is completed or merely attempted.

5.2 Customers, Counterparties, and Business Relationships

This Policy applies to **all customers, counterparties, and business relationships** of Fargo S.p.A., including:

- Natural persons
- Legal persons and other legal arrangements
- Intermediaries, agents, and introducers
- Occasional customers and long-term contractual counterparties.

The Policy applies both to the establishment of new relationships and to the ongoing management of existing relationships.

5.3 Directors, Employees, and Relevant Third Parties

This Policy is binding on:

- Members of the Board of Directors
- Senior management
- All employees, regardless of role or seniority
- Consultants, agents, and any third parties acting on behalf of Fargo S.p.A. or representing the Company in dealings with customers or counterparties.

Relevant third parties are required to comply with this Policy to the extent applicable to their role and are subject to appropriate oversight and contractual obligations.

5.4 Lifecycle of the Customer Relationship

This Policy applies throughout **the entire lifecycle of the customer relationship**, including:

- Pre-onboarding risk assessment and customer acceptance
- Customer onboarding and verification
- Ongoing monitoring and periodic review
- Enhanced due diligence where required
- Transaction execution and review
- Suspension, refusal, or termination of the relationship.

5.5 Contractual and Professional Obligations

Compliance with this Policy forms an **integral part of the contractual and professional obligations** of all individuals and entities subject to its scope. Failure to comply may result in disciplinary measures, contractual remedies, and, where applicable, legal consequences.

5.6 Cash Transactions Policy

Fargo S.p.A. recognises that cash transactions in the precious metals sector present an inherently elevated risk of money laundering and terrorist financing due to the anonymity, traceability limitations, and value density of cash and gold.

As a matter of policy, **Fargo S.p.A. does not accept cash payments or cash settlements for values above applicable statutory thresholds under Italian law** in connection with its business activities, including the purchase, sale, or transfer of precious metals.

Where, in exceptional and legally permissible circumstances, cash exposure cannot be avoided, such transactions shall:

- Be subject to **Enhanced Due Diligence (EDD)** irrespective of amount
- Require **prior written approval** from the Compliance Function and senior management
- Be supported by documented verification of the **source of funds** and the **economic rationale** of the transaction
- Be fully documented and subject to **enhanced transaction monitoring**
- Be assessed to determine whether the circumstances give rise to a **Suspicious Transaction Report (SOS)** obligation.

Any cash transaction exceeding applicable statutory thresholds, or presenting unusual characteristics, shall be refused or escalated without exception.

This policy reflects Fargo S.p.A.'s conservative risk appetite and its commitment to maintaining transparent, traceable, and regulator-acceptable transaction flows.

6. GOVERNANCE AND THREE LINES OF DEFENCE

Fargo S.p.A. adopts a structured governance framework to ensure effective oversight, accountability, and control of money laundering and terrorist financing risks. The Company's AML/CFT governance is based on the internationally recognised **Three Lines of Defence** model, which provides a clear allocation of responsibilities and ensures the independence of key control functions.

Ultimate responsibility for AML/CFT compliance rests with the **Board of Directors** of Fargo S.p.A.

6.1 First Line of Defence – Operational Functions

The First Line of Defence consists of all operational functions involved in the day-to-day execution of the Company's business activities.

Operational staff are responsible for:

- Applying Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) measures in accordance with this Policy and internal procedures
- Accurately collecting, verifying, and documenting customer and transaction information
- Understanding the customer's business profile, expected activity, and transaction behaviour

- Monitoring transactions and customer behaviour for consistency with known profiles
- Identifying unusual or suspicious activity and promptly escalating concerns to the Compliance Function
- Complying with sanctions screening, PEP identification, and other preventive controls.

Operational responsibilities are non-delegable and form part of each employee's professional and contractual obligations.

6.2 Second Line of Defence – Compliance Function

The Second Line of Defence is represented by the **Compliance Function**, headed by the **Responsabile Antiriciclaggio**, which operates independently from operational and commercial functions.

The Compliance Function is responsible for:

- Designing, implementing, and maintaining the AML/CFT framework of Fargo S.p.A.
- Developing and updating this Policy and related procedures
- Conducting and documenting AML/CFT risk assessments
- Overseeing the application of CDD, EDD, sanctions screening, and monitoring measures
- Assessing internal reports of suspicious activity and determining whether an SOS must be submitted to the UIF
- Providing guidance and support to operational staff
- Delivering and coordinating AML/CFT training programs
- Monitoring compliance with applicable laws, regulations, and internal policies
- Reporting periodically to senior management and the Board of Directors on AML/CFT matters, including risk exposure, deficiencies, and remediation actions.

The Compliance Function must be granted adequate authority, independence, access to information, and resources to perform its duties effectively.

6.3 Third Line of Defence – Independent Review and Audit

The Third Line of Defence consists of independent review and audit activities conducted either internally by a function independent from operations and compliance, or externally by qualified third parties.

Independent review and audit activities aim to:

- Assess the adequacy and effectiveness of the AML/CFT framework
- Verify compliance with Italian and EU AML/CFT requirements
- Test the effectiveness of CDD, EDD, transaction monitoring, and SOS processes
- Identify control weaknesses and areas for improvement.

Findings arising from independent reviews are documented and communicated to senior management and the Board of Directors. Fargo S.p.A. implements timely and proportionate remedial actions, which are tracked and subject to follow-up.

6.4 Role of the Board of Directors

The Board of Directors bears ultimate responsibility for AML/CFT governance and oversight. The Board shall:

- Approve this Policy and any material amendments
- Define the Company's AML/CFT risk appetite
- Ensure that adequate resources are allocated to AML/CFT compliance
- Oversee the effectiveness of the AML/CFT framework
- Review periodic AML/CFT reports and significant risk issues.

Board oversight and decision-making are documented to ensure traceability and accountability.

6.5 Escalation and Reporting Lines

Fargo S.p.A. establishes clear escalation and reporting lines to ensure that AML/CFT issues are addressed promptly and at the appropriate level.

- Operational staff escalate concerns to the Compliance Function
- The Compliance Function escalates material issues to senior management and, where appropriate, to the Board of Directors
- Urgent or high-risk matters may be escalated immediately, bypassing normal reporting cycles.

All escalations and decisions are documented and retained in accordance with record-keeping requirements.

7. DEFINITIONS AND INTERPRETATION

For the purposes of this Anti-Money Laundering and Counter-Terrorist Financing Policy, the following definitions shall apply. Where a term is not expressly defined in this section, it shall have the meaning attributed to it under **Legislative Decree No. 231/2007**, applicable European Union legislation, or established supervisory and regulatory practice.

These definitions shall be interpreted consistently throughout this Policy and any related procedures or annexes.

7.1 Anti-Money Laundering (AML)

Anti-Money Laundering (AML) refers to the body of laws, regulations, policies, procedures, and controls designed to prevent, detect, and deter the conversion or transfer of property derived from criminal activity, for the purpose of concealing or disguising its illicit origin or assisting any person involved in such activity to evade the legal consequences of their actions.

AML measures include, but are not limited to:

- Customer due diligence and identification requirements
- Monitoring and analysis of transactions
- Reporting of suspicious activity to competent authorities
- Record-keeping and audit trail requirements.

7.2 Counter-Terrorist Financing (CFT)

Counter-Terrorist Financing (CFT) refers to measures aimed at preventing the collection, provision, movement, or use of funds or other assets, directly or indirectly, with the intention that they be used, or in the knowledge that they will be used, to carry out terrorist acts or support terrorist organisations or individuals.

CFT obligations apply irrespective of whether the source of funds is lawful or unlawful and include enhanced scrutiny of transactions, customers, and geographic exposure linked to terrorism risk.

7.3 Beneficial Owner (Ultimate Beneficial Owner – UBO)

Beneficial Owner or **Ultimate Beneficial Owner (UBO)** means the natural person or persons who ultimately own or control a customer, or the natural person on whose

behalf a transaction or activity is conducted, in accordance with Articles 20–22 of Legislative Decree 231/2007.

Control may be exercised through:

- Direct or indirect ownership of a sufficient percentage of shares or voting rights
- Control through other means, including contractual arrangements or significant influence over management decisions.

Where no natural person can be identified through ownership or control, the beneficial owner shall be the natural person(s) holding senior management positions, in accordance with applicable law.

7.4 Business Relationship

Business Relationship means a professional or commercial relationship between Fargo S.p.A. and a customer which, at the time of establishment, is expected to have an element of duration. A business relationship may be formalised through contractual arrangements or arise through a series of related transactions.

Business relationships are subject to ongoing due diligence and monitoring throughout their duration.

7.5 Customer Due Diligence (CDD)

Customer Due Diligence (CDD) means the set of identification, verification, and monitoring measures applied by Fargo S.p.A. to:

- Identify and verify the identity of customers and beneficial owners
- Understand the purpose and intended nature of the business relationship
- Conduct ongoing monitoring to ensure that transactions are consistent with the customer's profile and risk classification.

CDD is applied on a risk-sensitive basis and constitutes a continuous process throughout the lifecycle of the customer relationship.

7.6 Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) refers to additional and more stringent due diligence measures applied in situations that present a higher risk of money laundering or terrorist financing.

EDD measures may include enhanced verification of identity, deeper analysis of ownership structures, verification of source of funds and source of wealth, senior management approval, and increased monitoring frequency.

7.7 Politically Exposed Person (PEP)

Politically Exposed Person (PEP) means a natural person who is or has been entrusted with prominent public functions, whether at domestic, foreign, or international organisation level, as well as their immediate family members and persons known to be close associates.

PEP status increases the inherent risk associated with a customer relationship and requires the application of enhanced due diligence measures in accordance with this Policy and applicable law.

7.8 Segnalazione di Operazione Sospetta (SOS)

Segnalazione di Operazione Sospetta (SOS) refers to a report submitted by Fargo S.p.A. to the **Unità di Informazione Finanziaria (UIF)** pursuant to Articles 35–41 of Legislative Decree 231/2007, where a transaction or behaviour gives rise to a reasonable suspicion of money laundering or terrorist financing.

SOS reporting obligations apply to both completed and attempted transactions and are subject to strict confidentiality and anti-tipping-off requirements.

8. ROLES AND RESPONSIBILITIES

Effective prevention of money laundering and terrorist financing requires a clear allocation of responsibilities, strong governance, and accountability at all levels of Fargo S.p.A. This section defines the roles and responsibilities of the governing bodies, management, compliance function, employees, and relevant third parties in relation to AML/CFT obligations.

8.1 Board of Directors

The **Board of Directors of Fargo S.p.A.** bears ultimate responsibility for ensuring that the Company complies with all applicable Anti-Money Laundering and Counter-Terrorist Financing obligations under Italian and European law.

In particular, the Board shall:

- **Approve this Policy** and any subsequent amendments, ensuring that it remains aligned with applicable legislation, regulatory guidance, and the Company's risk profile
- **Define and approve the Company's AML/CFT risk appetite**, taking into account the nature, scale, and complexity of the Company's activities in the precious metals sector

- **Ensure that adequate human, technical, and financial resources** are allocated to the implementation and maintenance of an effective AML/CFT framework
- **Oversee the effectiveness of the AML/CFT framework**, including the adequacy of internal controls, procedures, and systems
- **Receive and review periodic reports** on AML/CFT matters, including significant risk exposures, material compliance issues, internal control weaknesses, and Segnalazioni di Operazioni Sospette (SOS) activity
- **Promote a culture of compliance and integrity** throughout the organisation, setting the tone from the top.

Board oversight and decision-making in AML/CFT matters shall be **documented and demonstrable**, particularly for the purposes of supervisory inspections, external audits, and banking due-diligence reviews.

8.2 Senior Management

Senior management is responsible for implementing the directives and strategic guidance of the Board of Directors and for ensuring that AML/CFT policies and controls are effectively embedded in the Company's day-to-day operations.

In particular, senior management shall:

- Ensure that operational procedures and business practices are consistent with this Policy and applicable AML/CFT requirements
- Translate the Company's AML/CFT risk appetite into practical controls and processes
- Supervise operational functions to ensure proper application of CDD, EDD, monitoring, and escalation procedures
- Ensure that staff are adequately trained, supported, and supervised in the performance of AML/CFT-related duties
- Promptly escalate material AML/CFT issues to the Compliance Function and, where appropriate, to the Board of Directors.

Senior management plays a critical role in ensuring that AML/CFT compliance is not treated as a purely formal requirement, but as an integral part of the Company's operational decision-making.

8.3 Responsabile Antiriciclaggio (AML Compliance Officer)

Fargo S.p.A. appoints a **Responsabile Antiriciclaggio (AML Compliance Officer)** with sufficient authority, independence, and access to information to effectively discharge AML/CFT responsibilities.

The AML Compliance Officer is responsible for:

- **Developing, implementing, and maintaining** the Company's AML/CFT framework, including this Policy and related procedures
- **Conducting and periodically updating AML/CFT risk assessments**, taking into account changes in legislation, business activities, and risk exposure
- **Overseeing Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and ongoing monitoring** activities
- **Assessing internal reports of suspicious activity** and determining whether a Segnalazione di Operazione Sospetta (SOS) must be submitted
- **Submitting SOS reports to the Unità di Informazione Finanziaria (UIF)** in a timely and independent manner
- **Acting as the primary liaison** with competent authorities, including the UIF and supervisory bodies
- **Providing guidance and training** to staff on AML/CFT matters
- **Reporting regularly to senior management and the Board of Directors** on AML/CFT risks, compliance issues, and remediation actions.

The AML Compliance Officer must operate independently from commercial pressures and shall not be subject to undue influence in the performance of AML/CFT duties.

8.4 Employees and Relevant Third Parties

All **employees, consultants, agents, and relevant third parties** acting on behalf of Fargo S.p.A. are required to comply with this Policy and applicable AML/CFT procedures.

Their responsibilities include:

- Applying AML/CFT controls relevant to their role, including CDD and monitoring measures
- Remaining vigilant to unusual or suspicious activity
- **Promptly escalating any AML/CFT concerns** to the Compliance Function
- Participating in mandatory AML/CFT training programs
- Complying with confidentiality and anti-tipping-off obligations.

Failure to comply with this Policy may result in **disciplinary action, contractual remedies, and, where applicable, legal consequences.**

8.4.1 Agents, Intermediaries, and Introducers

Fargo S.p.A. may engage agents, intermediaries, or introducers in connection with its business activities. The Company recognises that such arrangements may present elevated AML/CFT risks if not properly controlled.

Accordingly, all agents, intermediaries, and introducers are subject to:

- **Mandatory Customer Due Diligence (CDD)** prior to engagement, including verification of identity, ownership, control, and business activities;
- **Written contractual undertakings** requiring compliance with applicable AML/CFT laws and Fargo S.p.A.'s internal AML/CFT policies;
- **Ongoing monitoring and periodic review**, proportionate to the nature and risk of the relationship;
- The Company's **right to audit**, request information, and conduct compliance reviews where necessary;
- Immediate **termination rights** in the event of AML/CFT breaches, non-cooperation, or unacceptable risk.

Agents and introducers are **strictly prohibited** from independently onboarding customers or establishing business relationships on behalf of Fargo S.p.A. without the Company's direct involvement and completion of full Customer Due Diligence by Fargo S.p.A.

Ultimate responsibility for customer acceptance, due diligence, and transaction approval **remains exclusively with Fargo S.p.A.**

9. MONEY LAUNDERING AND TERRORIST FINANCING RISK-BASED APPROACH

Fargo S.p.A. applies a **documented, structured, and proportionate Risk-Based Approach (RBA)** to the prevention of money laundering and terrorist financing, in accordance with **Articles 15–23 of Legislative Decree No. 231/2007**, the applicable European Union AML Directives, and relevant supervisory guidance.

The Risk-Based Approach ensures that the **nature, timing, and intensity** of AML/CFT measures applied by the Company are **commensurate with the level of risk identified**, allowing resources to be allocated efficiently while maintaining a high level of protection against financial crime.

9.1 Principles of the Risk-Based Approach

Fargo S.p.A. recognises that money laundering and terrorist financing risks are **not uniform** and may vary significantly depending on multiple interrelated factors. Accordingly, the Company does not apply a one-size-fits-all approach, but instead tailors its AML/CFT controls to reflect the specific risk profile of each customer and transaction.

The Risk-Based Approach is underpinned by the following principles:

- Identification and understanding of inherent money laundering and terrorist financing risks
- Application of proportionate and risk-sensitive controls
- Ongoing review and adaptation of controls in response to changes in risk
- Documentation and traceability of risk assessments and decisions.

9.2 Risk Factors Considered

In assessing AML/CFT risk, Fargo S.p.A. considers, at a minimum, the following categories of risk:

- **Customer risk**, including the customer's legal form, ownership and control structure, business activity, reputation, and PEP status
- **Geographic risk**, including the customer's country of residence, country of operation, source of funds, and involvement of jurisdictions identified as high risk by the European Union or other competent authorities

- **Product and service risk**, including the nature of precious metals transactions and any features that may increase vulnerability to misuse
- **Transaction risk**, including transaction size, frequency, complexity, and consistency with the customer's known profile
- **Delivery channel risk**, including the use of intermediaries, agents, or non-face-to-face relationships.

These risk factors are assessed both individually and in combination to determine the overall risk profile.

9.3 Timing of Risk Assessments

AML/CFT risk assessments are conducted:

- **Prior to establishing a business relationship**, as part of the customer onboarding and acceptance process
- **On an ongoing basis** throughout the lifecycle of the business relationship, through periodic reviews and transaction monitoring
- **Upon the occurrence of trigger events** that may materially affect the customer's risk profile, including changes in ownership, control, business activity, transaction behaviour, or geographic exposure.

9.4 Risk Classification and Mitigation

Based on the outcome of the risk assessment, customers and business relationships are classified into risk categories (e.g. low, medium, or high risk). The assigned risk classification determines:

- The level of Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) to be applied
- The frequency and depth of ongoing monitoring and review;
- Approval and escalation requirements.

Where higher risks are identified, Fargo S.p.A. applies enhanced controls and monitoring measures to mitigate residual risk to an acceptable level.

9.5 Documentation and Governance

All AML/CFT risk assessments, classifications, and related decisions are **fully documented** and retained in accordance with record-keeping requirements.

Risk assessment documentation is made available, upon request, to:

- Competent authorities

- External auditors
- Banking partners conducting due-diligence or compliance reviews.

The Risk-Based Approach is subject to oversight by the Compliance Function, senior management, and the Board of Directors, and is reviewed periodically to ensure continued adequacy and effectiveness.

10. CUSTOMER DUE DILIGENCE (CDD)

10.1 General Principles

Customer Due Diligence (CDD) constitutes the **cornerstone of Fargo S.p.A.'s AML/CFT framework** and is fundamental to the effective prevention and detection of money laundering and terrorist financing risks.

In accordance with **Articles 18–23 of Legislative Decree No. 231/2007**, Fargo S.p.A. applies CDD measures to ensure that it has an adequate and up-to-date understanding of its customers, the ultimate beneficial owners, and the purpose and intended nature of each business relationship.

CDD enables the Company to:

- Verify the identity of customers and beneficial owners
- Understand the customer's economic and business rationale
- Establish a baseline against which transactions and behaviour can be monitored
- Identify transactions or behaviours that deviate from expected patterns.

CDD measures are applied using a **Risk-Based Approach** and are proportionate to the level of risk associated with each customer, transaction, and business relationship.

10.2 Circumstances Requiring CDD

Fargo S.p.A. performs CDD measures in the following circumstances:

- **Prior to establishing a business relationship**, including contractual or ongoing commercial arrangements
- **Prior to carrying out an occasional transaction** exceeding applicable legal thresholds
- **Where there is a suspicion of money laundering or terrorist financing**, regardless of any thresholds or exemptions

- **Where there are doubts** about the accuracy, adequacy, or reliability of previously obtained customer identification or verification data.

As a general rule, CDD measures must be **completed before** the establishment of a business relationship or execution of a transaction.

Where **deferred verification** is permitted by law, such deferral shall:

- Be limited in scope and duration
- Not expose the Company to undue risk
- Be fully documented
- Be subject to prior approval by the Compliance Function.

10.3 Identification and Verification of Natural Persons

For **individual customers**, Fargo S.p.A. identifies and verifies, at a minimum, the following information:

- Full legal name
- Date and place of birth
- Nationality
- Residential address
- Tax identification number or equivalent identifier, where applicable.

Verification is performed using **reliable and independent source documents**, data, or information, including valid government-issued identification documents.

Where appropriate, additional verification measures may be applied to ensure the authenticity and validity of the information provided.

10.4 Identification and Verification of Legal Persons and Legal Arrangements

For **corporate and legal entity customers**, Fargo S.p.A. identifies and verifies, at a minimum:

- Legal name and registered office address
- Legal form and registration number
- Articles of association, constitutional documents, or equivalent
- Directors, legal representatives, and authorised signatories

- The existence and identity of the Ultimate Beneficial Owner(s).

Information is obtained from **official public registers**, corporate documentation, and other reliable and independent sources.

Where necessary, additional documentation is requested to ensure transparency and accuracy.

10.5 Beneficial Ownership Identification

Fargo S.p.A. identifies and verifies the **Ultimate Beneficial Owner(s)** of legal entities and arrangements in accordance with **Articles 20–22 of Legislative Decree 231/2007**.

Where ownership or control structures are complex, multi-layered, or opaque, enhanced analysis and additional documentation are required to ensure full traceability and transparency.

Where the beneficial owner cannot be satisfactorily identified or verified, Fargo S.p.A. shall **refuse to establish or continue** the business relationship and assess whether the circumstances give rise to a Suspicious Transaction Report.

10.6 Purpose and Intended Nature of the Business Relationship

As part of the CDD process, Fargo S.p.A. collects sufficient information to understand the **purpose and intended nature** of the business relationship, including:

- The nature of the customer's business, profession, or activity
- The expected level, volume, and frequency of transactions
- The source of funds and, where appropriate, the source of wealth.

This information forms the **baseline** for ongoing monitoring and risk assessment and is reviewed periodically to ensure continued relevance.

10.7 Ongoing Due Diligence and Monitoring

CDD is not a one-off exercise but an **ongoing process** throughout the lifecycle of the business relationship.

Fargo S.p.A. conducts ongoing monitoring to ensure that transactions and behaviour remain consistent with the Company's knowledge of the customer, including:

- Review and analysis of transactions

- Periodic updating of customer and beneficial ownership information
- Reassessment of the customer's risk classification
- Identification of unusual or suspicious patterns.

The frequency and depth of ongoing monitoring are proportionate to the assessed risk level.

10.7.1 Transaction Monitoring Framework

Fargo S.p.A. applies a structured transaction monitoring framework designed to detect unusual, inconsistent, or potentially suspicious activity throughout the lifecycle of the customer relationship.

Transaction monitoring is conducted through a combination of **manual and semi-automated controls**, proportionate to the Company's size, transaction volume, and risk profile.

Monitoring activities include:

- **Transaction-based monitoring**, conducted at the time of execution to assess consistency with the customer's known profile, expected activity, and stated purpose of the relationship
- **Ongoing periodic reviews**, conducted at frequencies determined by the customer's risk classification (e.g. low, medium, or high risk);
- **Trigger-event reviews**, initiated upon material changes in ownership, transaction behaviour, geographic exposure, or other risk-relevant factors.

Operational staff are responsible for the **first-level identification** of unusual activity, while the Compliance Function provides **second-level oversight**, independent assessment, and escalation where required.

The transaction monitoring framework is reviewed periodically by the Compliance Function to ensure its continued effectiveness and alignment with the Company's evolving risk profile.

10.8 Refusal, Suspension, and Termination of Relationships

Where Fargo S.p.A. is unable to complete CDD measures, identifies unacceptable risk, or detects inconsistencies that cannot be satisfactorily resolved, the Company shall, as appropriate:

- Refuse to establish the business relationship
- Suspend transactions or activities

- Terminate the business relationship.

All such decisions are **documented**, justified, and escalated to the Compliance Function. Where required, the circumstances are assessed for potential Suspicious Transaction Reporting obligations.

11. ENHANCED DUE DILIGENCE (EDD)

11.1 Purpose and Regulatory Basis

Enhanced Due Diligence (EDD) measures are applied by Fargo S.p.A. in circumstances that present a **higher risk of money laundering or terrorist financing**, requiring a level of scrutiny beyond standard Customer Due Diligence.

EDD is conducted in accordance with **Articles 24 and 25 of Legislative Decree No. 231/2007**, the relevant provisions of the European Union AML Directives, and applicable supervisory guidance.

The purpose of EDD is to obtain a **deeper and more comprehensive understanding** of:

- The customer and, where applicable, the beneficial owner(s)
- The ownership and control structure of the customer
- The **source of funds** used in transactions
- The **source of wealth**, where relevant
- The economic rationale and legitimacy of the transaction or business relationship.

EDD measures enable Fargo S.p.A. to identify, assess, and mitigate elevated risks and to determine whether the residual risk remains within the Company's approved risk appetite.

11.2 Circumstances Requiring EDD

EDD measures are applied, at a minimum, in the following circumstances:

- **Customers classified as high risk** under the Company's Risk-Based Approach, based on customer, geographic, transactional, or delivery channel risk factors
- **Business relationships involving Politically Exposed Persons (PEPs)**, including their family members and close associates
- **Transactions involving countries** identified by the European Commission or other competent authorities as **high-risk third countries**

- **Complex, unusually large, or non-standard transactions** that do not have an immediately apparent economic or lawful purpose
- **Situations involving complex, multi-layered, or opaque ownership or control structures**, including the use of intermediaries or nominee arrangements
- **Any scenario in which the nature, size, or pattern of transactions** appears inconsistent with the customer's known profile, business activity, or stated purpose of the relationship.

The presence of one or more of the above factors does not automatically require refusal of the relationship, but does require the application of appropriate EDD measures.

11.3 Enhanced Due Diligence Measures

EDD measures applied by Fargo S.p.A. may include, as appropriate and proportionate to the identified risk:

- Obtaining **additional identification and verification documentation** for the customer and beneficial owner(s)
- Verifying information using **independent, reliable, and, where possible, authoritative sources**, including public registers and reputable databases
- Establishing and verifying the **source of funds** used in specific transactions through documentary evidence
- Establishing and verifying the **source of wealth**, particularly where transaction values are significant or inconsistent with the customer's known profile
- Obtaining **explicit senior management approval** prior to establishing or continuing the business relationship
- Increasing the **frequency, scope, and depth of ongoing monitoring**, including transaction reviews and periodic reassessments
- Applying **transaction limits, additional controls, or specific conditions** on the relationship where necessary to mitigate risk.

All EDD measures applied are **fully documented**, justified, and retained in accordance with record-keeping obligations.

11.4 Senior Management Approval

Where EDD is required, the establishment or continuation of the business relationship is subject to **explicit approval by senior management**.

The approval process shall include:

- A documented assessment of the identified risks
- An evaluation of the effectiveness of proposed mitigating controls
- A determination that the **residual risk** is acceptable within the Company's AML/CFT risk appetite.

Senior management approvals and supporting documentation are retained and made available for audit and supervisory review.

11.5 Ongoing Enhanced Monitoring

Business relationships subject to EDD are monitored on an **enhanced and continuous basis**.

Enhanced monitoring includes, as appropriate:

- More frequent and detailed review of transactions and activity patterns
- Periodic reassessment of the customer's risk classification
- Regular updates of customer and beneficial ownership information
- Heightened scrutiny of deviations from expected behaviour.

The intensity of enhanced monitoring is adjusted dynamically in response to changes in the risk profile.

11.6 Failure to Satisfy EDD Requirements

Where EDD measures cannot be satisfactorily completed, or where the risks identified cannot be adequately mitigated, Fargo S.p.A. shall:

- Refrain from establishing the business relationship; or
- Suspend or terminate an existing relationship, as appropriate.

In such cases, the circumstances shall be assessed by the Compliance Function to determine whether they give rise to an obligation to submit a **Segnalazione di Operazione Sospetta (SOS)** to the Unità di Informazione Finanziaria (UIF).

All decisions and actions taken in relation to unsuccessful EDD outcomes are documented and retained.

12. POLITICALLY EXPOSED PERSONS (PEPs)

12.1 Regulatory Definition and Scope

For the purposes of this Policy, a **Politically Exposed Person (PEP)** is a natural person who is or has been entrusted with prominent public functions, in accordance with **Article 1, paragraph 2, letter dd) of Legislative Decree No. 231/2007**, the applicable EU AML Directives, and relevant supervisory guidance.

PEPs include, but are not limited to:

- Heads of State, Heads of Government, ministers and deputy or assistant ministers
- Members of parliament or similar legislative bodies
- Members of the governing bodies of political parties
- Members of supreme courts, constitutional courts, or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances
- Members of courts of auditors or the boards of central banks
- Ambassadors, chargés d'affaires, and high-ranking officers in the armed forces
- Members of the administrative, management, or supervisory bodies of state-owned enterprises
- Directors, deputy directors, and members of the board or equivalent functions of international organisations.

PEP status also extends to:

- **Immediate family members**, including spouses or partners, children and their spouses or partners, and parents; and
- **Persons known to be close associates**, including individuals with joint beneficial ownership of legal entities or close business relationships with a PEP.

12.2 Domestic, Foreign, and International Organisation PEPs

Fargo S.p.A. applies PEP measures to:

- **Domestic PEPs**
- **Foreign PEPs**
- **Persons entrusted with prominent public functions by international organisations.**

While all PEPs are subject to enhanced scrutiny, **foreign PEPs** and PEPs connected to jurisdictions presenting elevated corruption or governance risks are generally considered to present a higher inherent risk and are therefore subject to heightened attention and monitoring.

12.3 Identification and Screening of PEPs

PEP identification is conducted:

- At the time of customer onboarding
- On an ongoing basis through periodic screening of customers, beneficial owners, and relevant parties
- Upon trigger events, including changes in public office, ownership structure, or control.

Screening is performed using **reliable and reputable databases** and may be supplemented by open-source intelligence and other credible sources where necessary to confirm PEP status.

12.4 Due Diligence Measures for PEPs

Where a customer or beneficial owner is identified as a PEP, Fargo S.p.A. applies **Enhanced Due Diligence (EDD)** measures, including:

- Obtaining **explicit senior management approval** prior to establishing or continuing the business relationship
- Establishing and verifying the **source of wealth** and **source of funds**, with particular attention to consistency with the PEP's public function and known income
- Applying **enhanced and ongoing monitoring** of the relationship and transactions
- Increasing the frequency of periodic reviews and updates of customer information.

These measures are applied in a manner proportionate to the specific risk associated with the PEP relationship.

12.5 Cooling-Off Period and Risk Downgrading

In accordance with Italian and EU regulatory expectations, individuals who cease to be entrusted with prominent public functions shall continue to be treated as PEPs for a **minimum period of twelve (12) months** following the cessation of such functions.

Any decision to downgrade the risk classification after the cooling-off period shall:

- Be based on a documented risk assessment
- Take into account the level of influence still exercised by the individual
- Be approved by the Compliance Function.

Where residual risk remains elevated, enhanced measures may continue to be applied beyond the minimum cooling-off period.

12.6 Refusal, Suspension, and Termination of PEP Relationships

Where the risks associated with a PEP relationship cannot be adequately mitigated, Fargo S.p.A. shall refrain from establishing the business relationship or shall suspend or terminate an existing relationship, as appropriate.

Such cases shall be assessed by the Compliance Function to determine whether the circumstances give rise to an obligation to submit a **Segnalazione di Operazione Sospetta (SOS)** to the Unità di Informazione Finanziaria (UIF).

All decisions relating to PEP relationships, including approvals, refusals, and terminations, are documented and retained in accordance with record-keeping requirements.

13. SANCTIONS AND RESTRICTIVE MEASURES

13.1 Applicable Sanctions Framework

Fargo S.p.A. complies with all applicable **sanctions and restrictive measures** adopted by:

- The **European Union**, through directly applicable EU Regulations
- The **United Nations Security Council**

- The **Italian Republic**, through national implementing measures where applicable.

Sanctions and restrictive measures may include asset freezes, prohibitions on making funds or economic resources available, sectoral restrictions, trade embargoes, and other limitations imposed on specific individuals, entities, sectors, or jurisdictions.

Compliance with sanctions obligations is **mandatory and non-discretionary** and applies irrespective of any commercial considerations.

13.2 Sanctions Risk Exposure

Fargo S.p.A. recognises that its activities in the precious metals sector may be exposed to sanctions risk due to:

- Cross-border transactions
- International counterparties and supply chains
- Geographic exposure to jurisdictions subject to sanctions or restrictive measures.

Accordingly, sanctions compliance is fully integrated into the Company's AML/CFT risk management framework and Risk-Based Approach.

13.3 Sanctions Screening Procedures

Sanctions screening is conducted in a **systematic and risk-sensitive manner** and applies to:

- Customers and beneficial owners
- Directors, authorised signatories, and controlling persons
- Counterparties, intermediaries, and relevant third parties.

Screening is performed:

- **Prior to establishing a business relationship**
- **On an ongoing basis** through **periodic screening conducted at defined intervals**, and upon relevant trigger events.
- **Prior to executing transactions**, where appropriate.

Screening applies to customers, beneficial owners, directors, authorised signatories, counterparties, intermediaries, and relevant third parties.

Screening is conducted using **reliable and reputable databases**, supplemented where necessary by manual checks and open-source intelligence.

Responsibility for sanctions screening is shared between operational functions (first-level checks) and the Compliance Function (independent review, escalation, and decision-making).

The frequency and depth of sanctions screening are proportionate to the assessed risk and are reviewed periodically by the Compliance Function.

13.4 Handling of Potential Matches and False Positives

Where a potential sanctions match is identified, the matter is immediately escalated to the Compliance Function.

The Compliance Function shall assess whether the potential match constitutes:

- A **confirmed match**
- A **false positive**; or
- An **inconclusive result** requiring further investigation.

No transaction or activity shall be executed while a potential sanctions match remains unresolved. All assessments, decisions, and supporting documentation are fully documented and retained.

13.5 Confirmed Sanctions Matches

Where a **confirmed sanctions match** is identified, Fargo S.p.A. shall, without delay:

- Suspend or refuse the transaction or business relationship
- Refrain from making funds or economic resources available
- Comply with applicable notification and reporting obligations to competent authorities
- Implement any asset-freezing or restrictive measures as required by law.

All actions taken in response to confirmed sanctions matches are documented and retained.

13.6 Record-Keeping and Audit Trail

All sanctions screening activities, assessments, decisions, and outcomes are recorded and retained in accordance with statutory record-keeping obligations.

Records must be sufficient to:

- Demonstrate compliance with sanctions obligations
- Support internal and external audits
- Facilitate review by competent authorities and banking partners.

13.7 Training and Awareness

Relevant staff receive targeted training on sanctions obligations, including:

- Understanding applicable sanctions regimes
- Identifying sanctions risks
- Applying internal escalation procedures.

Sanctions training forms part of the Company's broader AML/CFT training program.

14. SUSPICIOUS TRANSACTION REPORTING (SOS)

14.1 Legal Obligation to Report

Fargo S.p.A. is subject to the obligation to report suspicious transactions in accordance with **Articles 35–41 of Legislative Decree No. 231/2007** and applicable EU AML legislation.

A **Suspicious Transaction** is any transaction, operation, attempted transaction, or behaviour that gives rise to a **reasonable suspicion** that the funds involved:

- Derive from criminal activity; or
- Are linked to terrorist financing; or
- Are intended to conceal or disguise the illicit origin of assets.

The obligation to report applies **regardless of the transaction amount**, the completion status of the transaction, or the existence of a business relationship.

14.2 Internal Identification of Suspicious Activity

All employees, consultants, agents, and relevant third parties acting on behalf of Fargo S.p.A. are required to remain vigilant and to actively identify unusual or suspicious activity.

Indicators of suspicious activity may include, but are not limited to:

- Transactions inconsistent with the customer's known business profile or financial capacity
- Unusual transaction structures or patterns lacking clear economic justification
- Reluctance or refusal by the customer to provide information or documentation
- Use of intermediaries or third parties without a legitimate rationale
- Attempts to structure transactions to avoid reporting or monitoring thresholds.

The presence of one or more indicators does not automatically require the submission of an SOS but does require further assessment.

14.3 Internal Escalation Procedures

Where an employee or relevant third party identifies suspicious activity, the matter must be **promptly escalated** to the Compliance Function without delay.

Internal escalation shall include:

- A description of the transaction or behaviour giving rise to suspicion
- Relevant customer and transaction details
- Supporting documentation and contextual information.

Internal reports are treated as strictly confidential and handled in accordance with internal procedures.

14.4 Assessment by the Compliance Function

The **Responsabile Antiriciclaggio** independently assesses all internal reports of suspicious activity.

The assessment takes into account:

- The customer's risk profile and classification
- Transaction history and behavioural patterns

- The economic rationale and consistency of the activity
- Any relevant external information, typologies, or alerts.

The assessment process must be objective, autonomous, and free from any commercial or operational influence.

14.5 Decision to Submit an SOS

Where, following assessment, the suspicion **cannot be reasonably excluded**, the Responsabile Antiriciclaggio shall submit a **Segnalazione di Operazione Sospetta (SOS)** to the **Unità di Informazione Finanziaria (UIF)** without delay, using the prescribed reporting channels.

The decision to submit an SOS:

- Is taken exclusively by the Compliance Function
- Does not require customer consent or approval from operational staff
- Must be documented, including the rationale for the decision.

14.6 Timing and Transaction Suspension

SOS reports must be submitted **promptly upon the formation of suspicion**.

Where execution of a transaction may interfere with investigative activities, Fargo S.p.A. shall suspend the transaction, unless such suspension is not feasible or may frustrate the purpose of the investigation.

Any decision to proceed with or suspend a transaction must be documented and justified.

14.7 Confidentiality and Prohibition of Tipping-Off

The existence, content, or submission of an SOS is subject to **strict confidentiality**.

Fargo S.p.A. strictly prohibits any form of **tipping-off**, including:

- Informing the customer or third parties that an SOS has been or may be submitted
- Disclosing information that could reasonably lead to the identification of an SOS.

Breaches of confidentiality and tipping-off prohibitions may result in **criminal liability** under Italian law.

14.8 Documentation and Record-Keeping

All internal reports, assessments, SOS submissions, and related documentation are recorded and retained securely in accordance with statutory record-keeping requirements.

Records must demonstrate:

- The decision-making process followed
- The independence of the assessment
- Compliance with legal and regulatory obligations.

Such records are made available to competent authorities and auditors upon request.

15. RECORD-KEEPING AND DATA RETENTION

15.1 Regulatory Basis and Objectives

Fargo S.p.A. maintains comprehensive AML/CFT records in accordance with **Article 31 of Legislative Decree No. 231/2007**, applicable European Union AML legislation, and relevant supervisory guidance.

The objectives of record-keeping and data retention are to:

- Ensure full **traceability and reconstruction** of customer relationships and transactions
- Enable timely access to information by competent authorities, auditors, and banking partners
- Support effective investigation and analysis of suspicious activity
- Demonstrate compliance with AML/CFT legal and regulatory obligations.

All records must be **accurate, complete, up to date, and reliable**, and maintained in a manner that ensures integrity, confidentiality, and availability.

15.2 Categories of Records Maintained

Fargo S.p.A. retains, at a minimum, the following categories of AML/CFT-related records:

- Customer identification and verification documentation collected under CDD and EDD

- Beneficial ownership information and supporting evidence
- Risk assessments, risk classifications, and related approvals
- Transaction records and supporting documentation sufficient to reconstruct individual transactions
- Internal reports of suspicious activity
- SOS assessments, submissions, and related correspondence
- PEP and sanctions screening results and assessments
- Records of senior management approvals
- AML/CFT training materials, attendance records, and effectiveness assessments
- Internal and external audit reports and remediation tracking documentation.

Records are maintained in a manner that allows for **clear linkage** between customers, transactions, decisions, and responsible personnel.

15.3 Retention Periods

All AML/CFT records are retained for a minimum period of **ten (10) years**, calculated from:

- The date of termination of the business relationship; or
- The date of execution of an occasional transaction.

Where required by law, regulatory instruction, or ongoing investigations, records may be retained for longer periods.

Upon expiry of the applicable retention period, records are securely destroyed or anonymised in accordance with applicable data protection requirements.

15.4 Storage, Security, and Access Control

AML/CFT records may be stored in **electronic and/or physical format**, provided that appropriate safeguards are in place.

Fargo S.p.A. implements technical and organisational measures to ensure that:

- Access to records is restricted to authorised personnel only, based on role and necessity

- Records are protected against unauthorised access, alteration, loss, or destruction
- Data integrity and confidentiality are preserved at all times
- Records can be retrieved promptly upon request by competent authorities.

Access rights are reviewed periodically to ensure continued appropriateness.

15.5 Data Protection and Confidentiality

The processing and retention of personal data for AML/CFT purposes are conducted in compliance with applicable data protection legislation.

Personal data collected for AML/CFT purposes:

- Is processed lawfully and fairly
- Is limited to what is necessary for compliance with legal obligations
- Is protected by appropriate security measures
- Is disclosed only to authorised parties and competent authorities.

Confidentiality obligations apply to all personnel with access to AML/CFT records.

15.6 Audit Trail and Traceability

Record-keeping systems must ensure a **complete and reliable audit trail**, enabling Fargo S.p.A. to demonstrate:

- The chronology of customer onboarding and verification
- The application of risk assessments and due diligence measures
- Decision-making processes, including approvals and escalations
- Transaction execution and monitoring activities
- SOS assessment and reporting actions.

The audit trail must be sufficient to support internal reviews, external audits, and supervisory inspections.

15.7 Availability to Authorities and Auditors

AML/CFT records are made available, upon lawful request, to:

- Competent Italian and European authorities
- The Unità di Informazione Finanziaria (UIF)
- External auditors and banking partners conducting due-diligence or compliance reviews.

Requests for access are handled promptly and in accordance with applicable legal and confidentiality requirements.

16. TRAINING AND AWARENESS

16.1 Training Objectives

Fargo S.p.A. recognises that effective AML/CFT compliance depends on the awareness, competence, and vigilance of its personnel. Training programs are designed to ensure that all relevant individuals understand their legal obligations, internal procedures, and the specific risks associated with the Company's activities in the precious metals sector.

Training supports the establishment of a strong compliance culture and enables timely detection and escalation of suspicious activity.

16.2 Scope of Training

AML/CFT training is mandatory for:

- Members of the Board of Directors
- Senior management
- Employees involved in customer onboarding, transaction processing, or monitoring
- The Compliance Function
- Any relevant third parties acting on behalf of the Company.

Training content is tailored to the role, responsibilities, and risk exposure of each category of personnel.

16.3 Training Content

Objectives of AML/CFT Training

Fargo S.p.A. recognises that the effectiveness of its AML/CFT framework depends not only on policies and procedures, but also on the **knowledge, awareness, and vigilance of its personnel**. AML/CFT training is therefore a core component of the Company's compliance framework and is designed to ensure that all relevant individuals understand their legal obligations and internal responsibilities.

The objectives of AML/CFT training are to:

- Promote a strong and consistent culture of compliance and ethical conduct
- Ensure awareness of applicable Italian and EU AML/CFT obligations
- Enable staff to identify, assess, and escalate suspicious activity effectively
- Reduce the risk of inadvertent non-compliance due to lack of knowledge or understanding.

Scope and Target Audience

AML/CFT training is mandatory for all individuals whose activities may expose Fargo S.p.A. to money laundering or terrorist financing risks, including:

- Members of the Board of Directors
- Senior management
- Employees involved in customer onboarding, transaction processing, monitoring, or compliance
- The Compliance Function
- Consultants, agents, and relevant third parties acting on behalf of the Company, where applicable.

Training requirements are **role-specific** and proportionate to the level of AML/CFT risk associated with each function.

Training Content

AML/CFT training programs are designed to be comprehensive and practical and cover, at a minimum:

- Overview of money laundering and terrorist financing risks relevant to the precious metals sector
- Italian and European AML/CFT legal and regulatory framework
- The Company's AML/CFT Policy and related internal procedures
- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) requirements
- Identification and handling of Politically Exposed Persons (PEPs)
- Sanctions and restrictive measures obligations
- Recognition of suspicious activity and internal escalation procedures
- Suspicious Transaction Reporting (SOS) obligations and anti-tipping-off requirements
- Record-keeping, confidentiality, and data protection considerations
- Consequences of non-compliance, including disciplinary and legal sanctions.

Training materials are periodically updated to reflect legislative developments, emerging risks, and supervisory expectations.

16.4 Frequency and Delivery Methods

AML/CFT training is provided:

- **Upon engagement or appointment** of new personnel
- **Periodically thereafter**, and at least on an annual basis
- **On an ad-hoc basis** where required by changes in legislation, business activities, or risk exposure.

Training may be delivered through:

- In-person training sessions
- Online or e-learning modules
- Targeted workshops or briefings
- Written guidance and internal communications.

The delivery method is selected based on the target audience, complexity of content, and operational needs.

16.5 Board and Senior Management Training

Members of the Board of Directors and senior management receive **tailored AML/CFT training** focused on:

- Governance and oversight responsibilities
- Risk appetite and strategic decision-making
- Interpretation of AML/CFT reports and risk indicators
- Personal accountability and potential liability under applicable law.

This ensures informed and effective oversight of the AML/CFT framework.

16.6 Documentation and Evidence of Training

Fargo S.p.A. maintains detailed records of all AML/CFT training activities, including:

- Training content and materials
- Dates and delivery methods
- Attendance and completion records
- Assessment results, where applicable.

Training records are retained in accordance with record-keeping requirements and made available to auditors and competent authorities upon request.

16.7 Assessment of Training Effectiveness

The effectiveness of AML/CFT training programs is periodically assessed through:

- Feedback from participants
- Knowledge assessments or testing
- Review of incidents, near misses, or audit findings
- Monitoring of escalation and reporting quality.

Identified gaps or weaknesses are addressed through targeted training enhancements or remedial actions.

16.8 Awareness and Ongoing Communication

In addition to formal training, Fargo S.p.A. promotes continuous AML/CFT awareness through:

- Internal communications and updates
- Circulation of regulatory alerts and guidance
- Compliance reminders and best-practice notices.

This ongoing communication supports sustained awareness and reinforces the importance of AML/CFT compliance in daily operations.

17. INDEPENDENT REVIEW, AUDIT, AND REMEDIATION

17.1 Independent Review Framework

Fargo S.p.A. subjects its AML/CFT framework to **periodic independent review** to ensure that policies, procedures, systems, and controls remain effective, proportionate, and fully aligned with applicable Italian and European AML/CFT requirements.

Independent reviews may be conducted:

- **Internally**, by a function that is organisationally and operationally independent from business and compliance operations; and/or
- **Externally**, by qualified third-party professionals with appropriate expertise in AML/CFT matters.

The independence, scope, and frequency of reviews are commensurate with the Company's risk profile and regulatory expectations.

The objectives of independent review are to assess:

- **Compliance with applicable laws and regulations**, including Legislative Decree No. 231/2007, EU AML Directives, and supervisory guidance
- **Effectiveness of AML/CFT controls**, including governance, due diligence, monitoring, and reporting mechanisms
- **Adequacy and consistency of policies, procedures, and systems**, taking into account the Company's business activities and risk exposure.

17.2 Scope and Methodology of Audits

AML/CFT audits and independent reviews may include, but are not limited to, the following activities:

- Review and validation of AML/CFT risk assessments and risk classifications
- Testing of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) files for completeness, accuracy, and consistency
- Evaluation of transaction monitoring processes, escalation mechanisms, and decision-making logic
- Review of Suspicious Transaction Reporting (STR) assessments, submissions, and documentation
- Assessment of sanctions and PEP screening processes
- Review of record-keeping practices and data retention controls
- Assessment of AML/CFT training programs, attendance, and effectiveness
- Evaluation of governance arrangements, reporting lines, and oversight mechanisms.

Audit methodologies may include sampling, walkthroughs, interviews, system testing, and documentation review.

17.3 Reporting of Findings

Findings arising from independent reviews and audits are **documented in formal reports** and communicated to:

- Senior management; and
- The Board of Directors, where findings are material or indicate elevated risk.

Audit reports typically include:

- Identified deficiencies or control weaknesses
- Assessment of the severity and potential impact of findings
- Recommendations for corrective action.

17.4 Remediation and Corrective Actions

Fargo S.p.A. implements **timely, proportionate, and risk-based remedial actions** to address deficiencies identified through independent reviews or audits.

Remediation actions may include:

- Updating policies and procedures
- Enhancing controls or systems
- Providing targeted training or guidance
- Strengthening governance or oversight mechanisms.

Each remediation action is assigned an owner, a target completion date, and clear deliverables.

17.5 Tracking and Follow-Up

Remediation actions are **tracked and documented** to ensure timely implementation and effectiveness.

Follow-up reviews are conducted to:

- Verify that corrective actions have been implemented as intended
- Assess whether identified deficiencies have been adequately addressed
- Confirm that residual risks have been reduced to an acceptable level.

The status of remediation actions is periodically reported to senior management and, where appropriate, to the Board of Directors.

17.6 Continuous Improvement

The outcomes of independent reviews, audits, and remediation activities are used to support **continuous improvement** of the Company's AML/CFT framework.

Lessons learned from audits, incidents, regulatory developments, and supervisory feedback are incorporated into:

- Policy updates
- Training programs
- Risk assessments
- Operational controls.

This continuous improvement cycle ensures that Fargo S.p.A.'s AML/CFT framework remains robust, effective, and aligned with evolving regulatory expectations.

18. POLICY REVIEW, GOVERNANCE CYCLE, AND CONTINUOUS IMPROVEMENT

18.1 Policy Review Cycle

This Anti-Money Laundering and Counter-Terrorist Financing Policy is subject to **regular and structured review** to ensure its continued adequacy, effectiveness, and alignment with applicable Italian and European AML/CFT legislation, supervisory guidance, and recognised best practices.

The Policy shall be reviewed:

- **At least annually**, as part of the Company's regular compliance cycle
- **Following material changes in legislation, regulations, or supervisory expectations**, including amendments to Legislative Decree No. 231/2007 or EU AML Directives
- **Upon significant changes in the Company's business model**, operational activities, products or services, geographic exposure, or customer base
- **Following material findings** arising from internal audits, external audits, supervisory inspections, or regulatory communications
- **In response to identified weaknesses or emerging risks**, including new typologies of money laundering or terrorist financing.

The review process ensures that the Policy remains proportionate to the Company's evolving risk profile and operational realities.

18.2 Governance and Change Management

Proposed amendments to this Policy are prepared by the **Compliance Function**, taking into account regulatory developments, audit findings, operational feedback, and risk assessment outcomes.

Amendments are subject to a structured governance process, which includes:

- Review by senior management to assess operational impact and implementation feasibility
- **Formal approval by the Board of Directors** for all material changes

- Clear documentation of the rationale for amendments and the expected compliance outcomes.

All versions of the Policy are:

- **Version-controlled**
- Clearly **dated**
- **Archived** in a secure and accessible manner.

This ensures full **traceability, accountability, and auditability** of the Policy lifecycle.

18.3 Communication and Implementation of Updates

Approved updates to the Policy are **communicated promptly** to all relevant personnel, including employees, management, and applicable third parties.

Communication methods may include:

- Internal circulars or memoranda
- Updated policy distributions
- Management briefings or compliance updates.

Where changes introduce new obligations or materially affect existing procedures, **targeted training or guidance** is delivered to ensure effective understanding and implementation.

The Compliance Function monitors the implementation of updates and addresses any identified gaps or issues.

18.4 Continuous Improvement

Fargo S.p.A. adopts a **continuous improvement approach** to AML/CFT compliance.

Feedback from:

- Policy reviews
- Audit and supervisory findings
- Operational experience
- Training assessments
- Emerging regulatory and risk developments

is systematically incorporated into updates of policies, procedures, controls, and training programs.

This continuous improvement cycle ensures that Fargo S.p.A.'s AML/CFT framework remains robust, responsive, and aligned with evolving regulatory expectations and industry standards.

19. ENTRY INTO FORCE AND BOARD APPROVAL

19.1 Entry into Force

This Anti-Money Laundering and Counter-Terrorist Financing Policy enters into force on the date of its formal approval by the **Board of Directors of Fargo S.p.A.**

From the effective date, this Policy:

- Replaces and supersedes any previous AML/CFT policies, procedures, or guidelines adopted by the Company
- Is binding on all directors, senior management, employees, consultants, agents, and relevant third parties acting on behalf of Fargo S.p.A.
- Applies to all existing and new business relationships and transactions, subject to applicable transitional arrangements where required by law.

19.2 Board Approval and Accountability

The Board of Directors formally confirms that it has:

- Reviewed the content of this Policy in full
- Assessed its adequacy in relation to the Company's business activities, risk profile, and regulatory obligations
- Approved the Policy as an appropriate and effective framework for the prevention of money laundering and terrorist financing.

The Board acknowledges its **ultimate responsibility** for AML/CFT compliance and commits to ensuring that:

- The Policy is effectively implemented across the organisation
- Adequate resources are allocated to support compliance
- Ongoing oversight of AML/CFT risks and controls is maintained.

19.3 Implementation and Oversight

Senior management, under the oversight of the Board of Directors, is responsible for ensuring the effective implementation of this Policy, including:

- Integration of the Policy into operational procedures
- Communication of obligations to relevant personnel
- Monitoring compliance and addressing deficiencies.

The Compliance Function supports implementation and reports periodically to senior management and the Board on the effectiveness of the Policy and any material issues.

19.4 Formal Approval Record

This Policy has been approved by resolution of the Board of Directors of Fargo S.p.A. as evidenced below:

Company: Fargo S.p.A.

Policy Title: Anti-Money Laundering and Counter-Terrorist Financing Policy

Date of Board Approval: _____

Effective Date: _____

Signed on behalf of the Board of Directors:

Name: _____

Title: _____

Signature: _____

ANNEX A

AML/CFT RISK ASSESSMENT METHODOLOGY

A.1 Purpose and Regulatory Context

This Annex sets out the **AML/CFT risk assessment methodology** adopted by Fargo S.p.A. to systematically identify, assess, mitigate, and document risks of money laundering and terrorist financing.

The methodology is designed and implemented in accordance with:

- **Articles 15–23 of Legislative Decree No. 231/2007**
- Applicable **EU AML Directives**
- Relevant supervisory guidance and recognised best practices.

This methodology underpins the Company's **Risk-Based Approach (RBA)** and ensures that AML/CFT controls are applied **proportionately**, consistently, and defensibly, based on the level of risk identified.

The risk assessment framework enables Fargo S.p.A. to:

- Identify inherent AML/CFT risks
- Apply appropriate mitigation measures
- Determine residual risk
- Allocate compliance resources effectively
- Demonstrate risk awareness to banks, auditors, and competent authorities.

A.2 Risk Assessment Framework

AML/CFT risk is assessed across **five core risk dimensions**, each of which reflects a recognised source of money laundering or terrorist financing risk:

1. **Customer Risk**
2. **Geographic Risk**
3. **Product / Service Risk**
4. **Transaction Risk**
5. **Delivery Channel Risk**

Each risk dimension is assessed **independently** and contributes to the overall risk profile of the customer or business relationship.

A.2.1 Risk Weighting Overview

To reflect the relative importance of each risk dimension, Fargo S.p.A. applies the following **risk weightings**, expressed as percentages of total inherent risk:

Risk Dimension	Weight (%)
Customer Risk	30%
Geographic Risk	20%
Product / Service Risk	20%
Transaction Risk	20%
Delivery Channel Risk	10%
Total	100%

This weighting reflects the Company's assessment that **customer and geographic factors** represent the most significant drivers of AML/CFT risk in the precious metals sector.

(In internal or presentation versions, this weighting may be represented graphically as a pie chart for clarity.)

A.3 Risk Scoring Scale

Each risk dimension is scored using a **three-level numeric scale**, designed to be simple, transparent, and auditable.

Score	Risk Level	Description
1	Low Risk	Minimal AML/CFT risk, strong transparency, low complexity
2	Medium Risk	Elevated but manageable risk requiring standard controls
3	High Risk	Significant AML/CFT risk requiring enhanced controls

Scores are assigned based on documented criteria and professional judgement, supported by evidence obtained during Customer Due Diligence.

A.4 Detailed Risk Dimensions

A.4.1 Customer Risk (Weight: 30%)

Customer risk assesses the inherent AML/CFT risk associated with the **nature, profile, and characteristics** of the customer.

Factors considered include:

- Customer type (individual, corporate, intermediary)
- Legal structure and complexity
- Beneficial ownership transparency
- Business activity and sector
- PEP status
- Reputation and adverse media.

Customer Risk Scoring Matrix

Risk Indicator	Low (1)	Medium (2)	High (3)
Customer Type	EU individual	EU corporate	Trust / complex entity
Ownership	Transparent	Multi-layered	Opaque / nominee
PEP Status	Not a PEP	Domestic PEP	Foreign / high-risk PEP
Business Sector	Regulated	Semi-regulated	High-risk / cash-intensive

A.4.2 Geographic Risk (Weight: 20%)

Geographic risk reflects the AML/CFT risk associated with **countries connected to the customer or transaction**, including:

- Country of residence or incorporation
- Country of operation
- Source of funds
- Destination of funds.

Geographic Risk Classification

Risk Level Description

Low (1) Italy, EU Member States, FATF-compliant jurisdictions

Medium (2) Third countries with improving AML regimes

High (3) EU-listed high-risk third countries or sanctioned jurisdictions

A.4.3 Product / Service Risk (Weight: 20%)

Product and service risk assesses the vulnerability of the Company's offerings to misuse for illicit purposes.

Factors include:

- Nature of precious metals transactions
- Liquidity and value density
- Ease of conversion or transfer
- Use of intermediaries.

Risk Level Description

Low (1) Standard, well-documented transactions

Medium (2) High-value or infrequent transactions

High (3) Structurally complex or unusual transactions

A.4.4 Transaction Risk (Weight: 20%)

Transaction risk evaluates the characteristics and behaviour of transactions over time.

Factors considered:

- Transaction size and frequency
- Consistency with customer profile
- Structuring or unusual patterns
- Third-party involvement.

Risk Level Description

Low (1) Predictable, consistent patterns

Medium (2) Occasional deviations

High (3) Unexplained, complex, or structured behaviour

A.4.5 Delivery Channel Risk (Weight: 10%)

Delivery channel risk assesses how the relationship is conducted.

Risk Level Description

Low (1) Face-to-face, direct relationship

Medium (2) Limited non-face-to-face elements

High (3) Fully remote or intermediated

A.5 Aggregate Risk Calculation

A.5.1 Inherent Risk Score

Each risk score is multiplied by its weighting to calculate the **weighted inherent risk score**.

Example Calculation (Illustrative):

Risk Dimension	Score	Weight	Weighted Score
Customer Risk	2	30%	0.60
Geographic Risk	1	20%	0.20
Product Risk	2	20%	0.40
Transaction Risk	2	20%	0.40
Delivery Channel	1	10%	0.10
Total Inherent Risk			1.70

A.5.2 Risk Classification Thresholds

Total Score Risk Classification

1.00 – 1.50 Low Risk

1.51 – 2.20 Medium Risk

2.21 – 3.00 High Risk

A.6 Mitigation Measures and Residual Risk

A.6.1 Mitigation Controls

Risk mitigation measures include:

- Standard CDD
- Enhanced Due Diligence (EDD)
- Senior management approval
- Enhanced transaction monitoring
- Transaction limits or conditions.

A.6.2 Residual Risk Definition

Residual risk represents the level of AML/CFT risk remaining **after** mitigation measures have been applied.

Residual risk is assessed to determine whether:

- The relationship may proceed
- Additional controls are required; or
- The relationship must be refused or terminated.

A.7 Review and Reassessment of Risk

Residual risk is reassessed:

- **At onboarding**
- **Periodically**, based on risk classification
- **Upon trigger events**, including:

Change in ownership or control

Change in business activity

Significant changes in transaction behaviour

Regulatory or geographic developments.

All reassessments are documented and retained.

A.8 Governance and Oversight

The AML/CFT risk assessment methodology is:

- Implemented by the Compliance Function
- Reviewed by senior management
- Subject to oversight by the Board of Directors
- Tested through independent audit and review.

This ensures that the methodology remains **effective, proportionate, and defensible**.

The following diagram provides a high-level visual representation of Fargo S.p.A.'s AML/CFT Risk Assessment and Control Framework. It illustrates the relationship between inherent risk factors, the effectiveness of mitigating controls, and the resulting residual risk, together with the corresponding strategic and tactical actions adopted by the Company. This framework underpins the Company's Risk-Based Approach and supports governance, oversight, and decision-making at all levels.



ANNEX B

CUSTOMER RISK CLASSIFICATION MATRIX

B.1 Purpose and Methodological Alignment

This Annex defines the **Customer Risk Classification Matrix** adopted by Fargo S.p.A. to assess and classify the inherent AML/CFT risk associated with customers and business relationships.

The matrix is an integral component of the Company's **Risk-Based Approach (RBA)** and operates in conjunction with the AML/CFT Risk Assessment Methodology set out in **Annex A**.

The objective of this matrix is to:

- Ensure **consistent and objective customer risk assessment**;
- Support proportionate application of CDD and EDD measures;
- Provide a transparent and auditable basis for risk classification decisions;
- Facilitate oversight by senior management, auditors, and banking partners.

B.2 Customer Risk Factors – Core Dimensions

Customer risk is assessed across **four primary qualitative dimensions**, which together represent the most significant indicators of money laundering and terrorist financing risk at customer level.

Each factor is scored independently using a **three-level scale (Low / Medium / High)**.

B.2.1 Customer Risk Factor Matrix

Factor	Low Risk (1)	Medium Risk (2)	High Risk (3)
Customer Type	EU-resident individual	EU corporate with simple ownership	Trusts, foundations, complex legal structures
Ownership & Control	Fully transparent, direct ownership	Multi-layered but identifiable	Opaque, nominee-based, or bearer arrangements
PEP Status	Not a PEP	Domestic PEP	Foreign or high-risk PEP
Business Activity	Regulated activity	Partially regulated	High cash exposure or unregulated sector

Each factor reflects a **recognised AML/CFT risk driver** identified in EU and FATF guidance.

B.3 Explanation of Customer Risk Factors

B.3.1 Customer Type

Customer type assesses the inherent risk associated with the **legal nature and complexity** of the customer.

- **Low Risk (1):**
Natural persons resident in the EU with straightforward financial profiles.
- **Medium Risk (2):**
EU-based corporate entities with simple ownership structures and identifiable management.
- **High Risk (3):**
Trusts, foundations, partnerships, or entities with complex or discretionary control mechanisms.

B.3.2 Ownership and Control Structure

Ownership risk evaluates the **transparency and traceability** of beneficial ownership.

- **Low Risk (1):**
Single-layer ownership with clear and verifiable beneficial owners.
- **Medium Risk (2):**
Multi-layer structures with identifiable beneficial owners after analysis.
- **High Risk (3):**
Opaque structures, nominee shareholders, or arrangements designed to obscure control.

B.3.3 Politically Exposed Person (PEP) Status

PEP risk reflects the **heightened corruption and abuse risk** associated with public office.

- **Low Risk (1):**
No PEP involvement.

- **Medium Risk (2):**
Domestic PEPs with limited influence and transparent income sources.
- **High Risk (3):**
Foreign PEPs or PEPs connected to high-risk jurisdictions or sectors.

B.3.4 Business Activity Risk

Business activity risk assesses the **susceptibility of the customer’s activity to misuse**.

- **Low Risk (1):**
Fully regulated and supervised activities.
- **Medium Risk (2):**
Partially regulated sectors with moderate exposure.
- **High Risk (3):**
Cash-intensive, high-value, or unregulated activities.

B.4 Geographic Risk Factors

Geographic risk assesses exposure arising from **countries connected to the customer or transaction**, including residence, incorporation, operations, and source of funds.

B.4.1 Geographic Risk Classification

Risk Level	Description
Low Risk (1)	Italy, EU Member States, FATF-compliant jurisdictions
Medium Risk (2)	Third countries with improving AML/CFT regimes
High Risk (3)	EU-listed high-risk third countries or sanctioned jurisdictions

Geographic risk is assessed in conjunction with customer and transaction factors.

B.5 Product / Service Risk

Product and service risk reflects the **intrinsic vulnerability of the products or services used**.

B.5.1 Product / Service Risk Classification

Risk Level	Description
Low Risk (1)	Standard, well-documented precious metals transactions
Medium Risk (2)	Large-volume or infrequent transactions
High Risk (3)	Structurally complex or unusual transactions

B.6 Aggregate Risk Scoring and Classification

B.6.1 Total Risk Score Calculation

Each risk factor is scored from **1 to 3**. The scores are aggregated to determine the **overall customer risk score**.

B.6.2 Risk Classification Thresholds

Total Score Risk Category

5 – 7	Low Risk
8 – 11	Medium Risk
12 – 15	High Risk

These thresholds are calibrated to ensure that elevated risk relationships are identified consistently and subjected to appropriate controls.

(In presentation or internal tools, this may be visualised using bar charts or colour-coded heat maps.)

B.7 Governance, Escalation, and Approval

B.7.1 Low and Medium Risk Relationships

- May be approved through standard onboarding procedures
- Subject to standard or proportionate monitoring
- Reviewed periodically based on risk classification.

B.7.2 High Risk Relationships

Business relationships classified as **High Risk** require:

- Application of **Enhanced Due Diligence (EDD)**
- **Explicit senior management approval** prior to establishment or continuation

- Enhanced and ongoing monitoring
- Documented justification of residual risk acceptability.

B.8 Documentation and Auditability

All customer risk classifications are:

- Fully documented
- Supported by evidence obtained during CDD and EDD
- Retained in accordance with record-keeping requirements
- Made available to competent authorities, auditors, and banking partners upon request.

The consistent application of this matrix supports transparency, accountability, and regulatory defensibility.

ANNEX C

CUSTOMER DUE DILIGENCE (CDD) & ENHANCED DUE DILIGENCE (EDD) DOCUMENTATION REQUIREMENTS

C.1 Purpose and General Principles

This Annex sets out the **minimum documentation requirements** for Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) applied by Fargo S.p.A., in accordance with **Articles 18–25 of Legislative Decree No. 231/2007**, applicable EU AML Directives, and supervisory best practices.

Documentation requirements are designed to ensure that:

- Customers and beneficial owners are properly identified and verified
- Ownership and control structures are transparent and traceable
- The source and legitimacy of funds and wealth are understood
- Records are sufficient to support audits, supervisory reviews, and banking due diligence.

All documentation collected must be:

- **Reliable, independent, and verifiable;**
- Proportionate to the assessed risk
- Kept up to date throughout the business relationship.

C.2 Natural Persons (Individuals)

C.2.1 Mandatory Documentation – Standard CDD

For **individual customers**, Fargo S.p.A. collects and verifies, at a minimum, the following documentation:

- **Valid government-issued identification document**, such as a passport or national identity card, containing a photograph and signature
- **Proof of residential address**, such as a utility bill, bank statement, or official correspondence, issued within an acceptable time frame
- **Tax identification number** or equivalent fiscal identifier, where applicable under national law.

These documents are used to establish the customer's identity, residency, and fiscal footprint.

C.2.2 Additional Documentation – Enhanced Due Diligence (EDD)

Where EDD is required, additional documentation may include:

- **Source of funds declaration**, detailing the origin of funds used in specific transactions or the business relationship
- **Source of wealth documentation**, such as employment income records, business ownership evidence, asset sale documentation, inheritance records, or investment statements
- **Enhanced screening results**, including adverse media, sanctions, and PEP screening outputs.

The objective of EDD documentation for individuals is to ensure that the customer's financial activity is **consistent with their known income, assets, and background**.

C.3 Legal Entities and Legal Arrangements

C.3.1 Mandatory Documentation – Standard CDD

For **corporate customers and other legal entities**, Fargo S.p.A. collects and verifies, at a minimum, the following documentation:

- **Certificate of incorporation or equivalent legal registration document**
- **Articles of association**, memorandum, or constitutional documents
- **Extract from the relevant official register**, such as the Chamber of Commerce or equivalent authority
- **Identification documents for directors, legal representatives, and authorised signatories**
- **Beneficial ownership declaration**, identifying the Ultimate Beneficial Owner(s) in accordance with applicable law.

These documents enable verification of the entity's legal existence, governance structure, and ownership and control.

C.3.2 Additional Documentation – Enhanced Due Diligence (EDD)

Where a legal entity is subject to EDD, additional documentation may include:

- **Group structure chart**, illustrating ownership and control relationships up to the ultimate beneficial owner(s);
- **Audited financial statements**, where available, or alternative financial information sufficient to understand the entity's economic activity;
- **Senior management approval documentation**, confirming that the relationship has been reviewed and approved in accordance with internal escalation requirements;
- Additional evidence supporting the **source of funds and source of wealth** of the entity and/or beneficial owners.

EDD documentation aims to address risks arising from **complex ownership structures, cross-border activities, or elevated risk profiles**.

C.4 Politically Exposed Persons (PEP) – Additional Requirements

Where a customer or beneficial owner is identified as a **Politically Exposed Person (PEP)**, Fargo S.p.A. applies additional documentation and control requirements.

Mandatory PEP-specific documentation includes:

- **Formal PEP declaration**, completed and signed by the customer
- **Detailed source of wealth verification**, supported by independent documentation
- **Evidence of senior management approval** for the establishment or continuation of the relationship.

PEP relationships are subject to **ongoing enhanced monitoring**, and documentation is reviewed and updated more frequently to reflect changes in risk profile.

C.5 Documentation Standards and Quality Controls

All CDD and EDD documentation must:

- Be clear, legible, and complete
- Be retained in a durable medium
- Allow for independent verification and reconstruction of the customer relationship.

Where documentation is incomplete, inconsistent, or unreliable, Fargo S.p.A. shall:

- Request additional information or clarification;
- Apply enhanced controls; or
- Refuse or terminate the business relationship, as appropriate.

C.6 Record-Keeping and Auditability

All documentation collected under this Annex is:

- Retained in accordance with statutory record-keeping obligations
- Linked to the customer's risk classification and due diligence file
- Made available to competent authorities, auditors, and banking partners upon request.

This ensures full **traceability, accountability, and regulatory defensibility** of CDD and EDD processes.

ANNEX D

SUSPICIOUS ACTIVITY INDICATORS AND TYPOLOGIES

D.1 Purpose and Use of Indicators

This Annex sets out a **non-exhaustive list of indicators and typologies** that may give rise to suspicion of money laundering or terrorist financing in the context of Fargo S.p.A.'s activities.

The indicators listed below are intended to:

- Assist employees and relevant third parties in recognising potentially suspicious behaviour or activity
- Support professional judgement in the identification and escalation of unusual transactions
- Provide a structured analytical framework for internal assessment.

The presence of one or more indicators **does not automatically require** the submission of a Segnalazione di Operazione Sospetta (SOS), but **must trigger further analysis and escalation** to the Compliance Function where appropriate.

D.2 Customer Behaviour Indicators

Suspicious activity may arise from **unusual or inconsistent customer behaviour**, particularly during onboarding or ongoing interactions.

Indicators include, but are not limited to:

D.2.1 Reluctance or Resistance to Disclosure

- Unwillingness or delay in providing required identification or documentation
- Objections to standard due diligence procedures without reasonable justification
- Attempts to negotiate or circumvent AML/CFT requirements.

D.2.2 Inconsistent or Misleading Information

- Information provided by the customer that is inconsistent with documentation or publicly available sources
- Frequent changes in explanations regarding the purpose of the relationship or transactions

- Contradictory statements regarding business activity, ownership, or source of funds.

D.2.3 Unusual Urgency or Pressure

- Attempts to pressure staff to complete transactions rapidly without adequate due diligence
- Claims of exceptional circumstances requiring immediate execution
- Disproportionate urgency that is not consistent with the nature of the transaction or relationship.

D.3 Transaction Pattern Indicators

Suspicious activity may also be identified through **transactional behaviour that deviates from expected patterns.**

D.3.1 Inconsistency with Known Customer Profile

- Transactions that are inconsistent with the customer's known business activity, financial capacity, or stated purpose of the relationship
- Sudden changes in transaction size, frequency, or nature without a clear economic rationale
- Use of products or transaction structures that are atypical for the customer.

D.3.2 Structuring and Threshold Avoidance

- Multiple transactions structured to remain below reporting or monitoring thresholds
- Repetitive transactions of similar amounts with no apparent business justification
- Fragmentation of transactions across different dates or accounts to avoid detection.

D.3.3 Third-Party Involvement

- Involvement of third parties without a clear or documented relationship to the customer
- Use of intermediaries where no legitimate commercial reason exists
- Payments made or received on behalf of unrelated parties.

D.4 Geographic Risk Indicators

Geographic factors may significantly increase AML/CFT risk and warrant enhanced scrutiny.

D.4.1 High-Risk Jurisdictions

- Transactions involving countries identified by the European Union as **high-risk third countries**
- Connections to jurisdictions subject to sanctions, embargoes, or other restrictive measures
- Countries with known deficiencies in AML/CFT frameworks.

D.4.2 Unnecessary Routing of Funds

- Funds routed through multiple jurisdictions without a clear economic rationale
- Use of offshore financial centres unrelated to the customer's business activity
- Complex routing of transactions designed to obscure the origin or destination of funds.

D.5 Combination and Escalation of Indicators

The assessment of suspicious activity should consider:

- The **number of indicators** present
- The **nature and severity** of the indicators
- The **context** of the customer relationship and transaction history.

Isolated indicators may not be sufficient to form a suspicion; however, **multiple indicators**, recurring patterns, or indicators combined with high-risk customer or geographic factors significantly increase the likelihood of suspicion.

D.6 Escalation and Assessment Process

Where indicators are identified:

- The matter must be **promptly escalated** to the Compliance Function
- Relevant information and documentation must be provided to support assessment

- The Compliance Function conducts an independent evaluation in accordance with internal SOS procedures.

Employees and relevant third parties must **not attempt to determine criminality**, but must focus on identifying and escalating unusual or suspicious activity.

D.7 Relationship with SOS Obligations

The identification of indicators under this Annex supports, but does not replace, the legal obligation to submit an SOS where suspicion cannot be reasonably excluded.

All assessments, decisions, and actions taken in response to suspicious indicators are documented and retained in accordance with record-keeping requirements.

ANNEX E

RECORD RETENTION SCHEDULE AND ACCESS CONTROLS

E.1 Purpose and Legal Basis

This Annex sets out the **record retention schedule** adopted by Fargo S.p.A. for Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) purposes.

Record retention is carried out in accordance with:

- **Article 31 of Legislative Decree No. 231/2007**
- Applicable European Union AML legislation
- Relevant supervisory and audit expectations.

The objectives of this retention framework are to:

- Ensure the **traceability and reconstructability** of customer relationships and transactions
- Enable timely access to information by competent authorities, auditors, and banking partners
- Support investigations into suspicious activity
- Demonstrate sustained compliance with AML/CFT obligations.

E.2 Record Categories and Retention Periods

Fargo S.p.A. retains AML/CFT records for a **minimum period of ten (10) years**, calculated from the termination of the business relationship or the execution of an occasional transaction, as applicable.

E.2.1 Retention Schedule

Record Type	Description	Retention Period
Customer Identification Data	Identification and verification documents collected under CDD and EDD	10 years
Beneficial Ownership Records	UBO declarations, ownership charts, verification evidence	10 years

Record Type	Description	Retention Period
Transaction Records	Documentation sufficient to reconstruct individual transactions	10 years
Risk Assessments	Inherent and residual risk assessments, classifications, approvals	10 years
SOS Documentation	Internal reports, assessments, SOS filings, UIF correspondence	10 years
PEP & Sanctions Screening	Screening results, assessments, escalation records	10 years
Training Records	Attendance logs, training materials, effectiveness assessments	10 years
Audit & Remediation Records	Audit reports, findings, remediation tracking	10 years

This retention schedule ensures consistency across all AML/CFT-related documentation.

E.3 Storage Format and Security Measures

AML/CFT records may be stored in **electronic and/or physical form**, provided that appropriate safeguards are in place to ensure:

- Confidentiality of sensitive and personal data
- Integrity and protection against unauthorised alteration or deletion
- Availability and prompt retrievability upon lawful request.

Fargo S.p.A. implements appropriate **technical and organisational measures**, including access controls, secure storage environments, and audit logging, to protect retained records.

E.4 Access Control and Authorisation

Access to AML/CFT records is strictly limited to **authorised personnel** on a need-to-know basis.

Authorised access may include:

- The Compliance Function
- Senior management, where relevant
- Internal or external auditors acting under mandate
- Competent authorities exercising lawful powers.

Access rights are reviewed periodically to ensure continued appropriateness and compliance with confidentiality obligations.

E.5 Confidentiality and Data Protection

All AML/CFT records are subject to strict **confidentiality obligations**.

Personal data contained in AML/CFT records:

- Is processed solely for compliance with legal obligations
- Is protected against unauthorised disclosure
- Is disclosed only to competent authorities, auditors, or banking partners where legally permitted.

E.6 Record Availability and Supervisory Access

AML/CFT records retained under this Annex are made available, upon lawful request, to:

- The Unità di Informazione Finanziaria (UIF)
- Other competent Italian or EU authorities
- External auditors and banking partners conducting due-diligence or compliance reviews.

Requests for records are handled promptly and documented to ensure traceability.

E.7 End of Retention Period and Secure Disposal

Upon expiry of the applicable retention period, AML/CFT records are:

- Securely destroyed; or
- Anonymised, where required by data protection considerations.

Disposal is carried out in a manner that prevents unauthorised access, reconstruction, or misuse of data.

E.8 Auditability and Governance Oversight

The record retention framework is:

- Overseen by the Compliance Function
- Subject to periodic review and audit
- Aligned with the Company's broader AML/CFT governance and risk management framework.

This ensures that Fargo S.p.A.'s record-keeping practices remain **defensible, proportionate, and regulator-ready**.

European Union AML Reform Package (AMLR / AMLA)

Fargo S.p.A. acknowledges the adoption at European Union level of the new Anti-Money Laundering and Counter-Terrorist Financing legislative framework, commonly referred to as the **EU AML Reform Package**, which includes, inter alia:

- **Regulation (EU) 2024/1624** on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the "AMLR"), which will be directly applicable in all Member States;
- **Directive (EU) 2024/1640** on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLD6); and
- **Regulation (EU) 2024/1620** establishing the **Anti-Money Laundering Authority (AMLA)**, with its seat in Frankfurt am Main, Germany.

Fargo S.p.A. recognises that the AMLR introduces a single, harmonised AML/CFT rulebook across the European Union, including enhanced and more prescriptive requirements in relation to customer due diligence, beneficial ownership transparency, cash transaction limits, sanctions compliance, and supervisory cooperation.

Although the Company is not currently classified as a directly supervised obliged entity under AMLA, Fargo S.p.A. acknowledges that its activities in the precious metals and gold sector may fall within the scope of **enhanced supervisory attention**, particularly in the context of cross-border operations and banking relationships.

Accordingly, Fargo S.p.A. commits to:

- Monitoring the implementation timelines and regulatory technical standards issued under the AMLR and AMLA framework;

- Assessing the impact of the EU AML Reform Package on its business model, internal controls, and compliance framework;
- Updating this Policy, related procedures, and internal controls in a timely manner to ensure continued alignment with directly applicable EU regulations and supervisory expectations; and
- Cooperating, where applicable, with competent national authorities, European supervisory bodies, and banking partners in relation to AML/CFT compliance under the new EU framework.

This Policy shall be interpreted and applied in a manner consistent with the objectives and principles of the EU AML Reform Package and shall be reviewed and amended as necessary to reflect the progressive entry into force of the AMLR, AMLD6, and AMLA-related requirements.