

Anti- Money Laundering Policy

ABSTRACT

Contents

1.	<u>OBJECT OF THE DOCUMENT AND SCOPE OF APPLICATION</u>	6
1.1	<u>KEY ACTIVITIES OF THE PARENT COMPANY AND RECIPIENT COMPANIES</u>	7
2.	<u>GLOSSARY</u>	10
3.	<u>LEGISLATIVE FRAMEWORK</u>	14
4.	<u>GENERAL PRINCIPLES AND OPERATING LIMITS</u>	15
5.	<u>INTERNAL ORGANISATION</u>	17
5.1	<u>PROPORTIONALITY PRINCIPLE</u>	17
5.2	<u>ROLES AND RESPONSIBILITIES OF THE CORPORATE BODIES</u>	17
5.2.1	<u>Strategic supervision body</u>	18
5.2.2	<u>Management body</u>	18
5.2.3	<u>Control body</u>	19
5.3	<u>ROLES AND RESPONSIBILITIES OF THE BUSINESS FUNCTIONS</u> <small>Errore. Il segnalibro non è definito.</small>	
5.3.1	<u>Anti-money laundering function</u>	20
5.3.2	<u>Head of anti-money laundering</u>	21
5.3.3	<u>Head of suspicious transaction reporting (STR)</u>	21
5.3.4	<u>Internal audit department</u>	23
5.3.5	<u>Business functions</u>	23
5.3.6	<u>Controlling business functions</u>	24
5.3.7	<u>Other business functions</u>	24
5.3.8	<u>Personnel</u>	24
6.	<u>MANAGEMENT OF ANTI-MONEY LAUNDERING AND TERRORIST FINANCING RISKS</u> <small>Errore. Il segnalibro non è definito.</small>	
6.1.	<u>GENERAL DUE DILIGENCE PRINCIPLES</u>	25
6.1.1	<u>Approach based on risk and customer profiling</u>	25
6.1.2	<u>Customer due diligence</u>	27
6.1.3	<u>Simplified due diligence procedures</u>	28
6.1.4	<u>Enhanced due diligence procedures</u>	30
6.1.5	<u>Updating of the due diligence</u>	33
6.1.6	<u>Constant control</u>	35
6.1.7	<u>Politically Exposed Persons (PEPs)</u>	36
6.1.8	<u>Relationships and transactions that involve high-risk third party countries</u>	37
6.1.9	<u>Remote provision of services/banking products</u>	38
6.1.10	<u>Performance of due diligence obligations by third parties</u>	39
6.1.11	<u>Abstention obligation</u>	40
6.1.12	<u>Relationships with trust companies</u>	40
6.1.13	<u>Pre-screening of potential customers and specific counterparties</u>	41
6.1.14	<u>“Passive KYC” and relations with institutional counterparties</u>	42
6.2	<u>SCOPE OF APPLICATION OF DUE DILIGENCE OBLIGATIONS</u>	43

6.2.1	<u>Factoring</u>	43
6.2.2	<u>Purchase of non-performing loans</u>	43
6.2.3	<u>Operating approach, including cross-border, to marketing banking products using digital platforms</u>	47
6.2.3.1	<u>Banking deposits offered to the customers of Raisin in Germany</u>	47
6.2.3.2	<u>Banking deposits offered to the customers of Banca Sella</u>	48
6.2.3.3	<u>Banking deposits offered to the customers of Hype</u>	48
6.2.4	<u>Life insurance products</u>	49
6.2.5	<u>Operating approach to the purchase and management of tax credits relating to construction, energy efficiency and the reduction of seismic risks (the “Superbonus” scheme)</u>	50
6.2.6	<u>Offer of Capital Markets Services</u>	51
6.2.7	<u>Real estate brokerage using online auctions</u>	52
6.2.8	<u>Retail brokerage of antiques and works of art using online auctions</u>	53
6.2.9	<u>Management of credit alternative investment funds set up for debt restructuring operations</u>	54
6.3	<u>MEANS OF COMBATING TERRORIST FINANCING</u>	57
6.4	<u>GENERAL PRINCIPLES ON THE RETENTION OF DATA AND INFORMATION</u>	58
6.5	<u>GENERAL PRINCIPLES OF INTERNAL CONTROL</u>	60
6.6	<u>SUSPICIOUS TRANSACTION REPORTING</u>	61
6.7	<u>OBJECTIVE COMMUNICATIONS</u>	62
6.8	<u>EMBARGO MANAGEMENT</u>	62
6.9	<u>CONTROLS ON FUND TRANSFERS</u>	63
6.10	<u>RESTRICTIONS ON THE USE OF CASH AND BEARER SECURITIES</u>	64
6.11	<u>RISK ASSESSMENT METHODOLOGY</u>	64
6.12	<u>TRAINING OF STAFF AND CONSULTANCY</u>	64
6.13	<u>WHISTLEBLOWING</u>	65
7.	<u>DISCIPLINARY MEASURES</u>	67
8.	<u>INFORMATION FLOWS TO THE SUPERVISORY BODY</u>	66
ANNEXES	67
ANNEX 1	67
ANNEX 2	83

This Policy establishes illimity's system of governance for combating money laundering and terrorist financing by way of a systematic and functional framework based on the Group's active collaboration in preventing these unlawful activities. Specific processes and procedures have been introduced for the obligations regarding a customer due diligence, suspicious transaction reporting, the retention of data and information, risk assessment and management, internal control and assurance of compliance with all the relevant provisions required to prevent and impede the occurrence of transactions connected with money laundering, terrorist financing and embargo violation.

The guidelines established in the Policy by the Parent Company are of a detailed nature and are to be implemented at every operating structure and subsidiary that is required to comply with anti-money laundering obligations - "Recipient Companies" - in proportion to the characteristics and complexity of the activities they perform, their size and organisational complexity, the type of services and products they provide and the features of their customer base, by:

1. establishing the strategic guidelines and policies needed for overall management of the money laundering risk at a Group level ("Group methodology for assessing money laundering risks");
2. having in place organisational systems and procedures suitable for ensuring compliance with the obligations for a customer due diligence, the identification and reporting of suspicious transactions and data retention;
3. establishing a clear definition of the roles, duties and responsibilities of each organisational unit;
4. setting up an anti-money laundering function as a control function specifically designated to oversee the prevention and management of money laundering risks;
5. carrying out constant control of compliance, by staff, of internal procedures and legal and regulatory requirements on anti-money laundering.

The business model distinguishes between activities in the following way for anti-money laundering purposes:

- a) disbursement of loans to SMEs, structured financing and acquisition financing operations – i.e. Crossover;
- b) factoring transactions;
- c) purchase of loans and/or new disbursements in the context of debt restructurings - i.e. Turnaround;
- d) purchase of corporate distressed debt – i.e. NPL and UTP loans;
- e) disbursement of credit and offer of other banking products to SMEs and POEs via a digital platform;
- f) purchase and management of tax credits;
- g) financing third parties for the purchase of secured non-performing loans by disbursing credit to securitisation companies formed pursuant to article 3 of Law no. 130/99 as amended - i.e. Senior Financing;
- h) offer of proprietary and third party banking services by way of a multichannel "Direct Bank" digital platform (web, app) www.illimitybank.com;
- i) cross-border offer of banking products in Germany via a digital platform operated by a third party (Raisin);
- j) distribution of life insurance products of a "term life policy" nature";
- k) collection of debt acquired under paragraph d) as well as on behalf of third parties pursuant to article 115 of the Consolidated Text of Laws on Public Security (*Testo Unico delle Leggi di Pubblica Sicurezza - TULPS*);
- l) real estate brokerage activity through online auctions which includes property repossessed through the enforcement of the mortgages securing the debt purchased under paragraph d);
- m) management of alternative investment funds (AIFs) set up with the aim of investment/divestment in receivables due from companies in temporary financial difficulty but with solid turnaround prospects and the restructuring of the debt of these companies with the possible issue of new finance.

Regarding the subjective perimeter, the above activities are followed by specific operating Areas in the Bank's Business Divisions or by the Recipient Companies.

Different customer segments are served and accordingly the size and extent of the applicable anti-money laundering laws and the relative obligations required to be met by the staff of the Bank and the Recipient Companies vary.

In accordance with the **risk-based approach** adopted by the Group, the intensity and extent of customer due diligence requirements are regulated on the basis of the degree of risk associated with each customer, applying either ordinary, simplified or enhanced due diligence procedures.

An assessment of the money laundering risk is made both at the initial stage, in order to discharge due diligence obligations, by assessing the elements identifying the customer, the executor or the effective owner in order to set up the ongoing relationship or carry out an occasional transaction, and throughout the whole contractual relationship, by examining transactions as a whole and checking and updating the data and information obtained in performing due diligence procedures.

The Parent Company adopts a **profiling model**, which enables it to automatically allocate a risk profile, through the use of IT procedures or *ad hoc* tools, on the basis of predetermined and uniform rationale and a scoring system. The Recipient Companies set up models that are consistent with the profiling model adopted by the Parent Company.

The Parent Company and the Recipient Companies carry out **constant control** by monitoring the evolution of the relationship and the customer's operations on an ongoing basis, also through the use of automated procedures, and if the suspicion of money laundering or terrorist financing should emerge, an internal **suspicious transaction reporting** procedure is activated in compliance with applicable laws and regulations.

In order to discharge data and information retention requirements, all the documents and information obtained during the performance of the customer due diligence procedures is kept for a period of ten years from the date of the termination of the ongoing relationship or execution of the occasional transaction. The Parent Company uses the Centralised Computer Archive (*Archivio Unico Informatico - AUI*) as a standardised archive and tool able to ensure compliance with laws and regulations on the retention of data information, and the Recipient Companies adopt systems for the retention of documents, data and information for combating money laundering and terrorist financing suitable for ensuring compliance with the provisions of article 32 of the Anti-Money Laundering Decree.