PicPay	POLICY	**Responsible Department:** Risk - AML/TF
		Classification: Extern
		Version: 02

ANTI MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING

1. Purpose

This Anti-Money Laundering and Counter Financing of Terrorism Policy ("Policy") aims to consolidate the established guidelines, define roles and responsibilities, establish governance, procedures, and disseminate knowledge on the topic of Anti-Money Laundering and Counter Financing of Terrorism within the companies PicPay Institution of Payment S.A., PicPay Bank - Banco Múltiplo S.A., PicPay Invest DTVM S.A., Crednovo SEP S.A., and all their respective subsidiaries (entities directly or indirectly controlled), hereinafter referred to as "PicPay Group", in addition to adopting a risk-based approach vision, as determined by the prevailing regulations.

This Policy aims to establish guidelines for the implementation of procedures and assignment of responsibilities, which aim to:

a) Identify, qualify, and classify customers appropriately and ensure complete verification of their information before initiating any commercial relationship or use of products and services. Exceptions should be dealt with in internal procedures provided they are in compliance with current regulations;
b) Adopt a risk-based approach to transaction monitoring and ensure the existence of controls, systems, and/or processes that allow for the identification, measurement, monitoring, management, and mitigation of money laundering and terrorism financing risks in a compatible manner;
c) Implement appropriate procedures to assess the risk of individuals, entities, countries, and activities, including regular verification of individuals and entities against all applicable international sanction lists, such as UN resolutions, OFAC, the European Union, and the United Kingdom;
d) Maintain monitoring and observation of the list of countries disseminated by competent authorities, considering those that are non-cooperative, have high levels of corruption, or have strategic deficiencies in implementing FATF recommendations;
e) Define procedures for reporting suspicious operations or circumstances of money laundering and terrorism financing to the competent public authorities;
f) Train and raise awareness, through periodic training, among the administrators and employees of the PicPay Group on Anti-Money Laundering and Counter Financing of Terrorism procedures.

2. Approval

This Policy is approved by the Conglomerate's Board of Directors.

Through this Policy, Senior Management reiterates its commitment to ensuring compliance with applicable legislation and regulations, as well as observing high ethical standards in conducting business and establishing and maintaining relationships with customers, partners and suppliers.

3. Applicability and Target Audience

This Policy applies, in Brazil and abroad, to the PicPay Group, as well as to all its administrators and employees, also including any interaction that the Conglomerate maintains with customers, partners, suppliers and other stakeholders.

4. Guidelines

The Anti-Money Laundering and Counter-Terrorism Financing Program of the PicPay Group aims to prevent its structure, products, or services from being involved in illicit activities. In this way, it protects not only its

reputation and image before its employees, customers, partners, suppliers, service providers, regulators, and society, but also ensures compliance with applicable laws and regulations.

5. Concepts

Money Laundering

The crime of Money Laundering is characterized by a set of commercial or financial operations that seek to incorporate into the economy, temporarily or permanently, resources, goods and values of illicit origin and that develop through a dynamic process that theoretically involves three independent phases that often occur simultaneously.

I - Placement is the stage in which the criminal introduces the amounts obtained illegally into the economic system through deposits, purchase of negotiable instruments or purchase of goods. Treat the removal of money from the place that was illegally acquired and its inclusion, for example, in the financial market.

II - Concealment aims to difficult the accounting/financial tracking of illicit resources, breaking the chain of evidence of the origin of this money, through the creation of complex layers of financial or non-financial operations, and conversion into other forms of investment, aiming to eliminate the origin and ownership of illegal funds.

III - In the **Integration** stage, the illegal resource definitively encompasses the economic and financial system. From this moment on, the money is given a legal appearance.

Money laundering always involves funds from illegal activities, while terrorist financing, discussed in the next section, comes from both legitimate sources of funding and funds from illegal activities.

Terrorist financing

Terrorist financing can be defined as the raising of funds in a legal or illicit manner and whose purpose is to allow groups or individuals to carry out activities aimed at imposing social or generalized terror, exposing people, property, peace and public security in danger.

Financing the Proliferation of Weapons of Mass Destruction

Financing can be defined as raising funds, whether lawful or illicit, and whose purpose is to allow groups or individuals, directly or indirectly, by any means, to provide financial support with the intention of being used for the proliferation of weapons of mass destruction, which may be biological, chemical or nuclear.

Sanction

Sanction is the restriction, in whole or in part, of carrying out commercial operations with a given country, individual and/or legal entity, established by a jurisdiction or by an international organization in retaliation for certain actions, adopted by the jurisdiction or sanctioned person, of an economic nature, political, social or warlike.

OFAC - Office of Foreign Assets Control

It is an agency integrated into the United States Department of the Treasury. Created in 1950, the OFAC's main responsibilities are administering and enforcing trade and economic sanctions, in accordance with the foreign policy and national security goals of the United States.

UNSC – United Nations Security Council

It is an agency of the United Nations whose mandate is to ensure the maintenance of international peace and security.

Politically Exposed Person - PEP

Politically Exposed Person ("PEP"): Politically exposed persons are public agents who perform or have performed in the last 5 (five) years, in Brazil or in countries, territories and foreign dependencies, positions, jobs or relevant public functions, as well as their representatives, family members and other people close to them. For clarification purposes, examples of situations that characterize a close relationship and entail the classification of a client as a politically exposed person are those people who have direct or indirect control of a legal entity created with the purpose of benefiting politically exposed persons.

Ultimate Beneficial Owner (UBO)

A natural person or persons who, individually or jointly, directly or indirectly, own, control, or significantly influence a legal entity or other similar structure, including representatives, attorneys-in-fact, and agents.

6. Procedures

Know Your Customer (KYC)

The "Know Your Customer" process refers to the actions taken to identify and qualify customers, through the collection, analysis, and storage of registration data, maintenance of the supporting documentation, identification of the corporate structure and ultimate beneficial owners, representatives and attorneys-in-fact, politically exposed persons, verification of the customer's origin, destination, and financial capacity, as well as procedures for updating customer records and checking for restrictions, in order to prevent the use of the company for illicit activities.

The verification and validation of identification information will be carried out according to each customer's profile and the nature of the business relationship, by cross-checking information with public and private databases. Information will be kept up to date according to the specific periodicity for each risk category.

Customers will be classified into risk categories as defined in the internal risk assessment, based on the information obtained during the customer identification and qualification procedures, the customer's risk profile, and the nature of the business relationship, and will be reviewed periodically.

The entire 'Know Your Customer' process, as well as special situations and restricted relationships, are specified in the Anti-Money Laundering and Counter-Terrorism Financing regulations, which are separated by each company within the PicPay Group.

Know Your Partner (KYP)

Identification and acceptance of business partners according to their profile and the purpose of the relationship, as well as assessing that they have appropriate anti-money laundering and counter-terrorism financing procedures in place, when applicable. Partners are considered to be all third-party service providers, business partners, and banking correspondents, when relevant to the business.

Know Your Supplier (KYS)

Identification and acceptance of suppliers and service providers, according to the profile and purpose of the relationship.

Know Your Employee (KYE)

In the know your employee process, procedures and controls are applied for the selection, hiring, and monitoring of the administrator and/or employee's status, including the activity performed, for the purposes of anti-money laundering, combating the financing of terrorism, and other illegal acts. These are guided by impartiality, ethics, transparency, and integrity, in accordance with the Code of Ethics and Conduct, internal policies, and current regulations, with no acts of discrimination being tolerated.

Monitoring, Selection, Analysis, and Reporting of Atypical Transactions

The transactions, including the use of products and services and/or transactions carried out, must be monitored with a focus on AML/CFT, through the establishment of internal rules and parameters consistent with current regulations.

The period for carrying out monitoring procedures and selecting suspicious transactions or situations must not exceed forty-five days from the date the transaction or situation occurred.

The period for carrying out the analysis procedures of selected transactions or situations must not exceed forty-five days from the date of selection of the transaction or situation.

Situations identified as atypical or suspicious are analyzed and, after deliberation, must be reported to the competent authorities and to COAF by the next business day.

Regardless of reporting to COAF, the analysis of cases must be formalized in a file and kept available for 10 years for national and international regulators.

All actions taken must be treated with absolute confidentiality, and it is forbidden to inform the involved clients or unauthorized third parties.

The process of monitoring and analyzing transactions and suspicious situations must be compatible with this Policy, defined based on the internal risk assessment, and must consider the identification of PEPs, including their representatives, relatives, and close associates, but not limited to these. These processes are specified in the PicPay Group's Anti-Money Laundering and Counter-Terrorism Financing regulations.

Analysis of unavailability of assets, rights and values

The PicPay Group has regulations in place for the analysis of the unavailability of assets, rights, and values owned, directly or indirectly, by individuals, legal entities, or entities with which we have or may have a business relationship, in compliance with Law Nº 13,810/2019.

Evaluation of New Products and Services

The implementation of new products and services, as well as their modifications, the use of new technologies, and distribution channels, must be evaluated by the Product Risk Assessment Committee, including an assessment from the perspective of anti-money laundering and counter-terrorism financing.

Training and Culture

Continuous actions are implemented to raise awareness among administrators, employees, outsourced service providers, and correspondents regarding the concepts of AML/CFT, definitions, regulatory requirements, the responsibilities of the company and its employees, and atypical situations that may lead to reports to COAF.

Internal Risk Assessment

The methodology to be used in the internal risk assessment will cover the risk profile of clients and the institution, including the business model and geographic area of operation, as well as operations, transactions, products, and services, encompassing all distribution channels and the use of new technologies, as well as the activities carried out by employees, partners, and outsourced service providers. Risk categories must be defined to enable the adoption of enhanced management and mitigation controls for higher-risk situations and the adoption of simplified controls for lower-risk situations.

Risk-Based Approach

The risk-based approach requires the cumulative assessment of all relevant risk factors, including the specific characteristics of customers, products, or services.

The assessment process will cover the classification of the active customer base by level of AML/CFT risk, segmented into risk categories defined in procedures.

Effectiveness Assessment

The effectiveness assessment of the AML/CFT Program must cover all existing processes regarding compliance with the policy, regulations, and internal controls. This assessment should be documented in a specific annual report, with a reporting date of December 31st, and submitted for review to the Audit Committee and the Board of Directors Committee of PicPay Group by March 31st of the year following the reporting date, in accordance with the minimum content defined by current regulations.

Confidentiality

In addition to the requirements provided for in the Code of Ethics and Conduct, it is prohibited to inform the client or third parties about communications made to the competent authorities, as well as any analyses carried out from the perspective of AML/CFT.

Communication Channel

Administrators, employees, suppliers, partners, and correspondents must immediately report situations with signs or evidence of illegal acts identified during prospecting, negotiation, or throughout the relationship using the following established channels:

Ethics Channel: https://www.canaldeetica.com.br/picpay/

7. Penalties

Failure to comply with AML/FT legislation and/or regulations, external or internal, will subject administrators, employees and the companies involved, as well as partners and/or suppliers, to penalties ranging from administrative to criminal, including fines, temporary disqualification from acting as a legal entity administrator, and revocation or suspension of the authorization to perform activities, operations, or business.

8. Final Considerations

The Anti-Money Laundering and Counter-Terrorism Financing Policy is essential to protect the PicPay Group from illegal activities and to ensure the integrity and transparency of its financial operations.

It is important that it is updated regularly to adapt to changes in legislation and to new threats related to money laundering and terrorism financing.

Effective implementation requires the commitment of top management and the collaboration of all employees and third-party service providers, who must be properly trained and made aware of these issues. In addition, constant monitoring and ongoing assessment of the risks and performance of the AML/CFT Policy are fundamental to ensure effectiveness and to guarantee that the PicPay Group is fulfilling its legal and ethical obligations.