AML COMPLIANCE NOTICE

Last Update: June 24, 2026

Novawave is a Digital Asset Service Provider (PSAD) registered with the National Commission of Digital Assets (CNAD) under Registration No. PSAD-0079 (20 April 2026), and a Bitcoin Service Provider (PSB) registered under the Bitcoin Law, Registration Code 6697f7c29c3ab49e3172b9f8 (29 July 2024).

Novawave S.A. DE C.V., with NIT: 0623-030624-109-2, located at Calle Cuscatlán, Casa #4312, Colonia Escalón, Distrito de San Salvador, San Salvador Centro, San Salvador, operating the web-platform https://monesy.io/ under the doing-business-name Monesy.io ("Monesy", "we") is unwavering in its commitment to combat money laundering, terrorist financing, and all forms of illicit activity. To this end, we have implemented the required framework of policies, procedures, and controls that align with industry standards and ensure compliance with effective anti-money laundering (AML), counter-terrorist financing (CTF), and Counter-proliferation of Weapons of Mass Destruction (CPWMD). These standards apply universally to all individuals and entities connected or affiliated with Monesy, including but not limited to our directors, statutory employees, independent contractors, consultants, agents, and partners.

All terms used in this Notice, not defined in this Notice, have the meanings outlined in the Terms of Services, our Privacy Notice, and El Salvador laws that are referred to in this Notice.

PURPOSE OF THE AML COMPLIANCE NOTICE

This AML Compliance Notice is designed to provide a brief overview of our AML-compliance practices and is not an exhaustive representation of Monesy's policies, procedures, and operational controls. This Notice represents an AML/CFT/CPWMD compliance framework for partners, clients, vendors, contractors, employees, regulatory authorities, law enforcement agencies, and other interested parties. It serves as an informational document to outline the principles and procedures that form our compliance efforts. Our internal stakeholders may access the full suite of policies and procedures for comprehensive guidance.

LEGAL FRAMEWORK

El Salvador's AML/CFT/CPWMD rules are set out in a range of legislative acts, including:

(a) Digital Asset Issuance Law, particularly Article 21, letter o), and Article 19
(b) Regulation of Digital Asset Service Providers

(c) Special Law for the Prevention, Control and Punishment of Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (Legislative Decree No. 426, 2025)
(d) Instructions for the Prevention, Detection, and Control of Money Laundering and Asset Laundering, Terrorist Financing, and Proliferation of Weapons of Mass Destruction issued by the Financial Investigation Unit (UIF)
(e) Special Law Against Terrorist Acts #108 (October 2006)
(f) Technical Rules (NRP-36) issued by the Central Reserve Bank of El Salvador
(g) CNAD Guide for Money Laundering and Terrorist Financing Risk Management
(h) Financial Action Task Force (FATF) 40 Recommendations
(i) United Nations conventions and international instruments

Monesy is committed to full compliance with the rules and requirements applicable to our operations as required by El Salvador laws and regulations. To meet these requirements, we constantly implement and improve our internal procedures and mechanisms designed to prevent money laundering and terrorist financing.

All data, including User identity information, is handled under Monesy's Privacy Notice and applicable data protection regulations securely and confidentially.

COMPLIANCE OFFICER

Monesy has appointed an official whose fundamental objective is to coordinate activities related to the prevention of money laundering (ML) and terrorist financing (TF) and the Proliferation of Weapons of Mass Destruction (PWMD) by:

(a) Overseeing the implementation and adherence to AML/CFT/CPWMD requirements
(b) Monitoring transactions for compliance with the policies and procedures for the prevention of ML/TF/PWMD
(c) Reporting transactions to the supervisory authority of El Salvador, where applicable
(d) Facilitating personnel training programs to enhance awareness and compliance

The Compliance Officer is independent and autonomous and has the power to make decisions relating to the exercise of his or her functions and obligations, in order to manage ML/TF/PWMD risks, in accordance with the provisions of applicable laws and regulations and a risk-based approach.

OBJECTIVES AND RESPONSIBILITIES FOR PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

To effectively identify and prevent money laundering and terrorist financing activities, Monesy is committed to maintaining a secure and compliant operational framework by executing the following responsibilities:

(a) Conducting comprehensive risk assessments related to ML and TF

(b) Developing and implementing policies, controls, and procedures to effectively mitigate and manage identified risks
(c) Applying KYC and KYB measures to verify and understand customer identities and activities
(d) Identifying and submitting transaction reports and documentation to the supervisory authorities in cases required by El Salvador rules and regulations
(e) Appointing a Compliance Officer responsible for implementing and providing applicable AML/CFT/CPWMD rules and procedures in Monesy
(f) Providing ongoing professional training to employees and maintaining regular internal oversight to ensure tasks are performed in alignment with compliance objectives
(g) Ensuring secure data storage and maintaining records as required by applicable laws and regulations
(h) Performing additional responsibilities and adhering to the requirements outlined in the applicable laws

IDENTIFICATION AND VERIFICATION OF OUR USERS

Monesy performs our Users' verification, which involves the implementation of procedures and controls to assess, identify, and verify the identity of our Users, whether natural or legal persons, and monitor their operations to manage and mitigate the ML/TF risks. Such identification and verification shall be conducted periodically and when required by this Notice and applicable laws.

Identification, depending on applicable customer due diligence procedure, as per individuals may include name, residential address, and other personal data; for legal entities may include identification of the legal form, name, economic activity, and identification of the entity's legal representative, persons with a shareholding of at least 10%, and members of the board of directors. In specific cases, for example, when a transaction exceeds set thresholds, when we find suspicious or unclear User behavior, or when we assume an escalation of risks, we will ask you to provide us with additional information and documents to mitigate the identified risks.

We may engage third-party service providers to facilitate the identification and verification procedures; however, Monesy retains full legal responsibility for ensuring compliance with established standards.

We take reasonable measures to carry out KYC/KYB processes, including the identification of Users in a reliable manner based on personal and entity identification documents and other information that is requested:

(a) At the time of contracting (when you create your Account or establish business relationships with us)
(b) For any occasional transaction of USD 1,000 (or equivalent) or more

(c) In case of any cash transactions totaling USD 10,000 (or equivalent) in aggregate per month, and all other transactions totaling USD 25,000 (or equivalent) in aggregate per month
(d) When there is uncertainty or discrepancy regarding the accuracy or validity of previously submitted information
(e) When there are reasonable grounds to suspect money laundering or terrorist financing involving the transaction, the User, the associated funds, or assets, regardless of the transaction's value
(f) In any other circumstances prescribed by applicable laws
(g) At any time at Monesy's sole discretion

TRAVEL RULE FOR VIRTUAL ASSET TRANSFERS

In compliance with El Salvador regulations and international standards (FATF Recommendation 16), Monesy implements the "Travel Rule" for all transfers of Digital Assets through our platform.

This applies to ALL virtual asset transfers regardless of transaction amount.

For every transfer of virtual assets, we collect and transmit the required information, including:

(a) Originator information (name, account identifier, address or identification)
(b) Beneficiary information (name, account identifier)
(c) Transaction details (date, type, and quantity of assets, addresses)
(d) Exchange rates used (if applicable)

This information is transmitted securely to receiving institutions and made available to regulatory authorities upon request. We screen all parties against sanctions lists before executing transfers.

We may reject, block, or delay transfers when required information cannot be obtained or when transactions raise compliance concerns.

RISKS MITIGATION

Monesy adheres to a risk-based approach for its AML/KYC procedures, evaluating and categorizing risks associated with each User. This approach considers multiple factors, including:

(a) Customer Risks (characteristics and behavior of the User)
(b) Geographical Risks (residence and/or location of Users, transactions, etc.)
(c) Product Risks (types of products, services, customers, and distribution channels)
(d) Other Risks that we find substantial

Risk assessments are conducted and updated periodically. Based on the results, Monesy reserves the right to take any measures required, such as requesting additional information or documentation, denying service provision, suspending access to the Platform, terminating the Account, or implementing further actions in compliance with applicable laws.

REPORTING

Monesy shall report all operations required to be reported in accordance with applicable laws and regulations to the controlling authority of El Salvador.

This includes both completed suspicious transactions and any attempts at suspicious transactions.

As a consequence of the proper implementation of Customer Due Diligence (CDD), we identify, document, and report to the Financial Investigation Unit (UIF) those operations that may be considered irregular, inconsistent, or unrelated to the client's type of economic activity.

RECORDS-KEEPING

Monesy shall keep documentation relating to the transactions, identification files, accounting files, and commercial correspondence of clients, as well as customers' due diligence-related data for a period of not less than fifteen (15) years. For transaction records, this period is counted from the date of finalization of each transaction; for customer identification data and account files, from the termination of the commercial relationship or closure of the account. Such data may not be deleted per the customer's request, because such retention is mandatory under applicable legal requirements (Article 26 of Legislative Decree No. 426/2025).

CONFIDENTIALITY AND NON-DISCLOSURE

In accordance with El Salvador laws and international standards, Monesy and our employees are prohibited from disclosing to customers or third parties that:

(a) A suspicious transaction report has been filed
(b) Information has been provided to the authorities
(c) A transaction is being reviewed for potential suspicious activity
(d) An investigation is being conducted or may be conducted

This confidentiality requirement protects the integrity of investigations and is required by law. Disclosure is only permitted when required by law, court order, or to authorized regulatory authorities.

POLITICALLY EXPOSED PERSONS (PEPS)

Business relationships with PEPs shall be evaluated on a case-by-case basis, factoring in associated risks and implementing enhanced due diligence measures where necessary. In certain situations, Monesy may be legally restricted, or at our discretion, may decide not to provide Services to PEPs.

RESTRICTED JURISDICTIONS

We shall not provide our Services to and will not establish business relationships with Users from territories and jurisdictions that are sanctioned or otherwise prohibited from being served by El Salvador laws, consider our Services officially unlawful, or that are not supportive per our own discretion.

We screen all users and transactions against applicable sanctions lists, including OFAC, UN Security Council, and FATF/GAFILAT high-risk jurisdictions.

DIGITAL ASSET SPECIFIC MEASURES

As a Digital Asset Service Provider, Monesy implements additional measures specific to virtual assets:

(a) Enhanced monitoring for transactions involving privacy coins or mixing services
(b) Risk assessment for transactions to/from self-hosted wallets
(c) Verification of stablecoin backing and issuer compliance
(d) Heightened scrutiny for cross-border digital asset transfers
(e) Monitoring of unusual transaction patterns specific to digital assets
(f) Immediate reporting of stablecoin admissions to CNAD as required by law

CONTACTS

For any concerns or inquiries regarding potential money laundering or terrorist financing, or if you have other questions and requests, please reach out to:

sp@monesy.io (attention: Compliance Officer)