enfinity® | energy for life

Anti-Money Laundering and Terrorist Financing Policy

December 17, 2021

1. Purpose of this Policy

At Enfinity Global Group we are strongly committed to the highest standards of business ethics, integrity and compliance. In particular, we are committed to actively preventing the use of Enfinity Global Group as a conduit for money laundering or terrorist financing.

It is Enfinity Global Group's approach to conduct business with legitimate Business Partners (defined below) whose funds are deriving from legitimate activities only. Enfinity Global Group does not accept any money laundering or terrorist financing activities and seeks to avoid that any of its business activities are misused for such criminal purposes. Enfinity Global Group fully supports government-sponsored measures to combat money laundering and terrorist financing.

The purpose of this Anti-Money Laundering and Terrorist Financing Policy (the "Policy") is to provide a general framework to prevent money laundering and terrorist financing in Enfinity Global Group's business activities and in all countries where Enfinity Global Group operates. The requirements set forth in this Policy shall be observed and, when needed, implemented by means of specific procedures.

2. Scope and Application

This Policy is mandatory and extends to all Enfinity Global Group entities worldwide. Thus, all Professionals of the Enfinity Global Group shall comply with the provisions of this Policy, regardless of the position they hold and territory where they are located.

If the applicable local anti-money laundering and anti-terrorist financing regulations are stricter than those of this Policy, such provisions shall be complied with and their violation will also be considered a violation of this Policy.

3. Definitions

Anti-money Laundering Documents	Anti-Money Laundering Documents include transaction records, know your client information and any other information regarding anti-money laundering controls.
Blacklisted Subject	An individual, entity, person or place that exists on a list of names that are screened to identify sanctions or export controls exposure, in addition to government and vendor-maintained sanctions lists. Other potential additions to a blacklist may come from government agency advisories and

	other warnings that list entities are considered high risk from a money laundering, terrorist financing, or sanctions evasion perspective. Blacklists are maintained by a number of countries and entities including the European Union, United Nations, United States of America, Financial Action Task Force, and World Bank.
Business Partners	Business Partners include any individual, company or organization, regardless of location, that is in contact with any Enfinity Global Group Professional or entity, or with whom any Enfinity Global Group Professional or entity establishes contact, with the purpose of initiating or continuing any potential business relationship.
Business Transactions	Any bids, quotes, projects, work orders, contracts (including employment, services, agency, or other contracts), payments, shipments, exports or reexport and any additional types of business activities.
Cash	Physical currency, bonds, cheques, or anything equivalent to cash.
Enfinity Global Group	Enfinity Global Inc. and its majority-owned and majority-controlled subsidiaries and affiliates.
Professionals	Employees and other persons working for Enfinity Global Group, regardless of the type of contractual relationship with Enfinity Global Group. Thus, it includes employees at all levels, whether permanent or temporary, full or part time, freelance contractors, managers, officers, directors, as well as any other secondees or contractors under Enfinity Global Group's effective control, regardless of the territory where they are located.
Supervisory Body	Enfinity Global Group's Supervisory Body.

4. What is money laundering and terrorist financing?

In short, money laundering is a method of concealing the origins of money gained through illegal activities, which is itself a crime, and returning that illegal money to ordinary use. Thus, money laundering includes, among others, the following:

(i) **Placement** - acquiring, converting or transmitting goods knowing that they proceed from the commission of a crime, thus placing criminal proceeds into the regular financial system;

(ii) **Layering** - performing acts that aim to hide or conceal the illegal origin;

(iii) **Integration - Justification** - hiding or concealing the origin, location, destination or movements of the goods knowing their illicit origin, to create an apparent legal origin of the money;

(iv) **Integration - Investment** - using money derived from criminal activities for the personal benefit of criminals or to intensify criminal activities like terrorism; and

(v) **Accomplices, Accessories, and Conspiracies** - cooperating with those who have committed the crime to help them avoid the consequences of their actions.

Terrorist organizations vary widely, ranging from large, state-like organizations to small, decentralized and self-directed networks. Terrorist financing mechanisms reflect this diversity. Financing is required not just to fund specific terrorist operations, but to meet the broader organizational costs of developing and maintaining a terrorist organization and to create an enabling environment necessary to sustain their activities.

5. General commitments

Enfinity Global Group is committed to:

1) Complying and acting in compliance with applicable anti-money laundering and anti-terrorist financing laws.

2) Facilitating that Enfinity Global Group's Professionals understand this Policy and carry out business on behalf of Enfinity Global Group in a legal, ethical and professional manner, according to applicable anti-money laundering and anti-terrorist financing laws.

3) Monitoring and punishing any conduct contrary to this Policy.

4) Maintaining effective mechanisms to encourage Enfinity Global Group’s Professionals to raise concerns in good faith, or on the basis of a reasonable belief, in confidence, and without fear of reprisal.

5) Effectively implementing this Policy through appropriate training and other controls.

6. Requirements

6.1. Payments

a) Cash payments

With the exception of petty cash, Enfinity Global Group avoids making and receiving payments in cash. If a Professional needs to make or receive one or various cash payments above USD 500 or equivalent, it shall request prior approval from the Enfinity Global Group CFO.

b) Making payments

Payments to suppliers can only be made to bank accounts under the name of said supplier, in the country where the supplier is operating or where the products or services were supplied. Enfinity Global Group shall request in the relevant markets proof of ownership of the bank account provided by the supplier. The full name of the payment addressee needs to be included in the payment form and file.

c) Receiving payments

Payments from our counterparties shall be made from bank accounts under the name of said payor. Otherwise, Enfinity Global Group shall request sufficient evidence from the counterparty regarding the relationship between payer and counterpartyand the appropriateness of this payment arrangement. If a payment is received from a country considered a tax haven or a non-cooperative jurisdiction for tax purposes by the US, the EU or other relevant authorities, the relevant Professional will contact the Legal Department.

d) Actions when a change of bank account is identified or requested

When a change of bank account is identified or requested, the following actions need to be taken before making payment:

(i) Confirm the change with the Business Partner;

(ii) In the relevant markets, ask for the new account bank ownership certificate issued by the bank.

6.2. Verification of Business Partners

a) Verification of new Business Partners

Enfinity Global Group's Professionals are required to properly identify and verify a Business Partner prior to commencing a new business relationship in accordance with internal policies and procedures, such as the Enfinity Global Group "Know Your Supplier Policy".

b) Verification of existing Business Partners

Existing Business Partners may also be periodically reviewed according to their risk and its relationship with Enfinity Global Group.

6.3. Verification of Business Transactions

a) Verification of new Business Transactions

Professionals are required to fully understand the purpose, process and rationale for any new, and especially new kind, of Business Transaction prior to commencing a new, or expanding an existing, business relationship. Professionals should be suspicious if the type, structure, process or economic outcome of a Business Transaction is not in line with good business judgment or the contract's terms.

b) Verification of ongoing Business Transactions

Ongoing Business Transactions may be periodically reviewed to identify changes to transactions or transaction structures that would raise any of the red flags referred to in Section 6.4 below.

6.4. Actions when positive result occurs upon verification

Where:

- any of the aforesaid verifications or checks lead to a positive result (e.g., a red flag) with respect to money laundering or terrorist financing;
- the verification did not produce a hit, but a Professional suspects a Business Partner is associated with Blacklisted Subjects; or
- questions, concerns or suspicions arise regarding Cash and bank transactions and/or money laundering or terrorist financing in general,

Relevant Enfinity Global Group Professionals are required to immediately contact the Legal Department.

If there is any suspicion of money laundering or terrorist financing in business relations with a validated Business Partner, that suspicion must be escalated to the Legal Department and that business (including the making or accepting of payments or delivery of goods/services) must be suspended immediately, until further guidance by the Legal Department.

Any suspended business relation may only be continued after approval by the Supervisory Body.

6.5. Red Flags

In order to prevent money laundering, Enfinity Global Group's Professionals shall act properly upon red flag indicators that a transaction or business may be suspicious. Thus, upon identifying a red flag, a Professional shall discuss the issue with its superior and, in case of doubts, with the Legal Department.

Identifying the possibility of anti-money laundering and anti-terrorist financing regulations violations in respect of a Business Partner or Business Transaction is often difficult. The risks can vary depending on the nature, scope, locations and parties involved in a transaction or business, as well as market practices and customs.

Typical red flags include the following:

- A counterparty or supplier is reluctant to provide standard information about its identity, nature of business, its management, shareholders, beneficiaries, prior banking relationships or sources of payment;
- There is little to no online information available regarding the counterparty or supplier, or the nature of its business;
- A counterparty or supplier has been recently established, has significant financial resources at its disposal and it is unclear how it came into possession of these financial resources or has assets well in excess of its known income;
- The counterparty or supplier Business Partner is uncommon to Enfinity Global Group's business in profession, education, business type, or business origin;
- The counterparty or supplier requests wire transfers to or from a different country than where the transaction occurs or where the company is headquartered, particularly if located without a reasonable explanation in an offshore bank secrecy or tax haven;
- The payment terms or method of payment are unusual (e.g., the counterparty is willing to pay a large amount in cash immediately (non-bank transfers));
- The transaction structure is atypical, or far more complex or rushed than necessary, for the business proposed;
- The Business Transaction appears to be improvident or inefficient, to lack business sense, economic substance, or apparent investment strategy and therefore may only be explained by a suspicion of some illicit activity like money laundering;
- The counterparty is offering to pay prices well over normal market value for the goods or services concerned;
- A counterparty or supplier insists on using banks that are not well known, or cash or cash equivalents only or cryptocurrency;

- A counterparty or supplier suggests payment transactions outside of the standard banking system (i.e., Black Market Peso Exchanges, Hawala, barter transactions, etc.);
- The counterparty appears to be structuring the transaction to have payments fall immediately below a certain amount to avoid a reporting or recordkeeping requirement;
- The counterparty provides unusual or suspicious identification or financial documents that cannot be readily verified;
- The counterparty requests that funds be transferred to or from an unrelated third party without providing adequate justification;
- Business Transactions contemplated are with, or for the benefit of, politically exposed persons (e.g., individuals that hold a prominent public position or function like government officials, political party officials, senior government executives, or their close family members or associates);
- The transaction involves counterparties located in countries subject to OFAC sanctions or identified as supporting international terrorism (https://sanctionssearch.ofac.treas.gov/);
- The counterparty or supplier is located in a country or is a financial institution identified as being of "primary money laundering concern" (https://www.fincen.gov/reg_section311.html);
- The counterparty is located or has accounts or financial dealings in countries either identified as being non-cooperative with international efforts against money laundering by the Financial Action Task Force (https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)) , or against whom the US Treasury Department has issued an advisory (https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information).

This is not intended to be an exhaustive list. Contact the Legal Department with any questions.

7. Document retention

Enfinity Global Group shall endeavor to keep appropriate records with respect to specific Anti-money Laundering Documents during and for five years following the conclusion of the business relationship in order to fulfill legal requirements, to provide evidence in the case of disputes, and to preserve information which has historic value.

8. Final Provisions

8.1 Administration and implementation

This Policy is an internal document of the Enfinity Global Group. It has been adopted on behalf of the Enfinity Global Group for its sole use and benefit. This Policy shall be administered on behalf of the Enfinity Global Group by the Supervisory Body.

There are no third parties who have any right to rely on the terms of this Policy, nor do any third parties have the right to enforce the terms of this Policy. None of Enfinity Global, any member of the Enfinity Global Group, nor any officer, director, employee, agent, or affiliate of any of the foregoing, shall be required to account to, or otherwise inform or notify, any third parties with respect to the matters described in this Policy.

8.2 Approval and amendment of this Policy

This Policy has been approved by the Supervisory Body. The Supervisory Body shall have the sole and exclusive right to amend, waive, terminate, or otherwise modify the terms of this Policy, whether directly or indirectly, and in any specific case or generally.

8.3 Dissemination

All Enfinity Global Group's Professionals are individually required to read, understand and comply with this Policy.

The Supervisory Body shall adopt the appropriate measures to ensure that this Policy is available and known to all Professionals to be complied and adhered to this internal regulation.

8.4 Interpretation

The Supervisory Body shall have the sole and exclusive right and duty to construe and interpret the terms of this Policy, and all such constructions, interpretations and decisions by the Supervisory Body shall be final and binding on all persons and entities whatsoever.

8.3 Non- compliance and reporting irregularities

Enfinity Global Group does not tolerate violations of this Policy. Failure to comply with this Policy, or falsification of documentation required to be created or maintained under this Policy, will result in appropriate disciplinary action, which, depending on the circumstances, may include termination of employment or of a commercial relationship.

Any Enfinity Global Group Professional who has reason to suspect a breach of this Policy must promptly bring such to the attention of the Supervisory Body.

Adopted December 17, 2021