

# Anti-Money Laundering and Counter-Terrorism and Sanction Policy

Version: Initial 1.0

Effective Date: 16 December 2023

This Anti-Money Laundering and Counter-Terrorism and Sanction Policy (the **AML Policy**) is an integral part of the General Terms of Service (the **Terms**) [\[LINK\]](#). This AML Policy outlines NM FINANCE LTD's (the **Company**) objectives and tasks as well as rules relating to the prevention and combating of money laundering and terrorism and proliferation financing.

## 1. DEFINITIONS AND ABBREVIATIONS

1.1. This AML Policy uses the same definitions as the Terms, unless otherwise specified herein.

The AML Policy also employs some additional definitions:

- 1.1.1. **TF** – Terrorist Financing
- 1.1.2. **ML** – Money Laundering
- 1.1.3. **PF** – Proliferation Financing
- 1.1.4. **KYC** – Know-Your-Customer
- 1.1.5. **EUR** – Euro
- 1.1.6. **USD** – USA Dollar
- 1.1.7. **EU** – European Union
- 1.1.8. **AML** – Anti-money Laundering
- 1.1.9. **CTF** – Counter-terrorism Financing
- 1.1.10. **CDD** – Customer due diligence
- 1.1.11. **Cooperation partner** – natural or legal person, legal entity or association of such persons/entities from which the Company receives services or potentially plans to do so;
- 1.1.12. **International sanctions** – restrictions imposed according to the international law in relation to subject of sanctions, which have been adopted by the United Nations Organization or the European Union, United Kingdom or another international organization, of which the respective Marine Insurance Services group company is a member state, and which are enforced in the respective country of operations of the Marine Services group company in question;
- 1.1.13. **Subject of the sanctions** – a subject of public international law, a natural or legal person, or another identifiable subject on which international or national sanctions have been imposed;
- 1.1.14. **Sanctions risk** – the impact and probability that the Company may be used to violate or circumvent sanctions;
- 1.1.15. **SumSub** – Sum and Substance Ltd, company number 09688671, Registered office address: 30 St. Mary Axe, London, England, EC3A 8BF <https://sumsub.com/>.

## 2. PURPOSE OF THE AML POLICY

2.1. The purpose of the the Company's AML Policy is to set the principles and approach of the Company to determine the measures which are applied to identify, assess, manage the AML/CTF and sanctions risks that are inherent to the Company and to implement

appropriate processes to mitigate such risks to protect the Company, the Customers, and our business partners from the risks of ML/TF and sanctions.

- 2.2. The Company is committed to preventing, detecting and deterring money laundering and terrorist financing and has a zero-tolerance policy regarding ML/TF and sanctions. To that end, it is the responsibility of every employee (including contract and part-time employees) to comply with this AML Policy.

### **3. OBJECTIVE AND TASKS**

- 3.1. The Company when conducting its activity in the national and international business environment, recognizes risks existing in the world resulting from the committed and possible acts of terrorism worldwide, legalization of illegally obtained funds and organized crime that endangers the social, political, economic and legal policy and stability of democracy and civilization. The Company wishes to perform its activity in a way to secure itself against the risk of being involved in possible money laundering and terrorism financing and being involved in violation of restrictions of the applicable national and international sanctions.
- 3.2. The objective of this AML Policy is:
  - 3.2.1. to conduct business activities in conformity with the applicable legislation and international requirements regulating actions and conduct in AML/CTF area;
  - 3.2.2. to protect the Company from the risk of being involved in possible money laundering and terrorist financing and the risk of violating restrictions of the applicable national and international sanctions;
  - 3.2.3. to minimize the possibility to cooperate with the clients, Talents and business partners whose activities fail to comply with the applicable legislation and international requirements regulating actions and conduct in AML/CTF area and this AML Policy; and
  - 3.2.4. to protect the Company from potential losses arising from non-compliance with applicable legislation and international requirements governing actions and conduct in AML/CTF and sanctions areas, ensuring the preservation of the Company's reputation and the maintenance of confidence in the Company.
- 3.3. To achieve the objectives outlined in Clause 2.1, the Company shall undertake the following actions in its activities:
  - 3.3.1. observe, fulfil, and introduce in its activity requirements of laws and international legislation, recommendations and guidelines issued by authorities which are binding upon the Company;
  - 3.3.2. draft and implement internal regulatory documents, procedures, instructions, and other internal regulations as required by law and ensures control over compliance with such internal regulations;
  - 3.3.3. ensure sufficient financial, material and human resources to comply with this AML Policy;
  - 3.3.4. train its staff in the sphere of AML/CTF and observance of sanctions regimes, compliance with the legislation and implementation of this AML Policy;
  - 3.3.5. implement in its daily activity principles set forth in this AML Policy;
  - 3.3.6. control compliance with this AML Policy.
- 3.4. The Company defines/stipulates:

- 3.4.1. written internal policies, procedures to ensure compliance with the binding AML/CTF laws and regulations, and controls;
- 3.4.2. identification and due diligence requirements of Talents;
- 3.4.3. unacceptable relationships;
- 3.4.4. sanctions to be observed by the Company;
- 3.4.5. the personnel training requirements and awareness;
- 3.4.6. record keeping requirements;
- 3.4.7. review of policies and procedures on a regular basis;
- 3.4.8. implementation of the AML Policy, control over its execution;
- 3.4.9. responsibility for non-compliance with the AML Policy and its breaches.

## **4. REGULATORY FRAMEWORK**

- 4.1. The Company shall establish and maintain effective and adequate AML/CTF internal control systems that will be designed to comply with:
  - 4.1.1. applicable AML/CTF legal and regulatory requirements and other legal requirements that are binding upon the Company in question;
  - 4.1.2. international organizations' AML/CTF recommendations, standards, guidelines and "best practices" principles.
- 4.2. As part of AML/CTF compliance efforts the Company shall ensure that the Company complies with applicable national and international financial sanctions regulations.

## **5. UNACCEPTABLE TALENTS, KEY PRINCIPLES OF DUE DILIGENCE**

- 5.1. The Company is prohibited from maintaining anonymous Accounts for Talents or Accounts registered under obviously fictitious names. We are also prohibited from executing Earnings Balance payouts on behalf of anonymous or fictitious Talents. In the Protocol, Talents may use pseudonyms or nicknames different from their verified names; however, the Company must always verify their identities and provide Services exclusively to verified Talents.
- 5.2. The Company shall not accept Users' money that is known or suspected to be the proceeds of criminal activity.
- 5.3. The Company shall not approve cooperation with a Talent if it possesses information indicating a possible connection of the Talent with money laundering/terrorist financing (ML/TF), fraudulent, or other illicit activities;
- 5.4. The Company shall not establish any business relationship with a Talent, if the Talent is unable or refuses to complete the CDD requirements, including identifying and verifying the identity;
- 5.5. The Company shall not establish a relationship with individuals known or suspected to be terrorists or a criminal organization, or member of such, or listed on Sanction lists;
- 5.6. The Company shall not establish any relationship with the Talent, if they are citizens and residents of internally prohibited country (Annex 1).
- 5.7. The Company may apply additional restrictions on what type of Users they do or don't accept from ML/TF risk perspective.

## **6. SANCTIONS REGIME AND NO SERVICES TO SANCTIONED PERSONS**

- 6.1. The following international and national sanctions are binding upon the Company:
  - 6.1.1. United Nations (UN) sanctions;
  - 6.1.2. EU sanctions;
  - 6.1.3. Office of Foreign Assets Control (OFAC) sanctions.
- 6.2. The Company shall not provide services to persons that are subject to the international or national sanctions.
- 6.3. Before establishing a relationship with the Talent, the Company shall screen them against the Sanction list and perform ongoing sanction screening and monitoring.

## **7. VERIFICATION OF THE TALENT**

- 7.1. During registration of the Talent Profile, the Talent must undergo identity verification performed by the third-party provider, SumSub (<https://sumsub.com/>). This process is aimed at ensuring safety, security, and integrity for users by minimizing the risks of fraud, money laundering, and other illegal activities.
- 7.2. According to the terms of the contract, SUM AND SUBSTANCE LTD provides the following services, including making available the analysis of the images and information contained therein in order to check the personal data in the databases and receive reports with the results of such analysis:
  - 7.2.1. Document integrity check;
  - 7.2.2. A solution for automatically extracting data from documents
  - 7.2.3. Face Match control;
  - 7.2.4. Verification of identity documents (Determines the authenticity and legitimacy of a document to ensure that it has not been falsified or altered)
  - 7.2.5. Checking Watchlists, including whether the person is on a global sanctions list, PEP list, Adverse media etc.
  - 7.2.6. Additional checks, including completeness of documents, cross-check of all submitted documents (name, date and place of birth, signature), identity (online photo of customer vs information in submitted document).
- 7.3. When verifying the identity of the Talent, using Protocall, the Talent must provide an e-mail address, which will be verified immediately.
- 7.4. During the identification process, the Talent presents an identity document in real time using the SumSub solution (the customer receives a link, using it he is asked to show the document to the camera on the phone in real time and a photo of the customer is taken in real time). At this stage, the passport or ID cards photo is checked to see if the person matches. If for any reason the Talent sends a photo of the document in manual mode (downloads from the platform or sends it by e-mail), the file must not have been modified/edited/updated by special computer programs (automatically checked by SumSub). Photographs of documents and Talent must be legible and the following information must be clearly legible: the person's first and last name; date of birth and/or personal identification number, photograph and/or facial image, the person's signature, the expiry date and number of the document, the name of the issuing authority, nationality and place of birth. The document must be complete and must not be tampered. In addition to the identity document, the customer takes a photo of their face in the SumSub platform in the online mode and takes the photo with the presented identity document in their hand (a

so-called selfie). Also, SubSum performs a “liveness check” to ensure, that photo of the face is made by real person in real time.

- 7.5. For identity verification purposes the Talent (private individual) provides identity document (passport or ID card).
- 7.6. After talent verification, the Company conducts a profile moderation process in which an employee reviews the description of the proposed service and the type of activity of the talent to check for compliance with prohibited services (Annex 2). Users have the option to report a service and prohibited content. As part of the complaint process, the Company conducts a re-moderation of the Talent's profile, and in case prohibited content is detected, the Talent's profile should be suspended or terminated, depending on the severity of violation.
- 7.7. As part of the daily screening, the Company performs daily checks of existing Talents against various external databases using the SumSub name check, including daily checks to see if the person is or was recently added to any global sanctions list, if the person is or recently was a PEP or if the person is on a watch list or blacklist. The SumSub system is based on a risk-based approach and follows a global database.

## **8. VERIFICATION OF THE USER**

- 8.1. The Company verifies the identity of the User if the User initiates a deposit in form of Talking Balance for an amount exceeding 1000 euros per transaction, or if the total sum of multiple apparently related transactions is 15,000 euros or more, or if the transaction involves a foreign currency that, based on the exchange rate used for accounting at the start of the transaction day, is equal to or exceeds 15,000 euros.
- 8.2. The User's identity is verified by the third-party provider SumSub (<https://sumsub.com/>).
- 8.3. During the identification process, the User presents an identity document in real time using the SumSub solution (the customer receives a link, using it he is asked to show the document to the camera on the phone in real time and a photo of the customer is taken in real time). At this stage, the passport or ID cards photo is checked to see if the person matches. If for any reason the User sends a photo of the document in manual mode (downloads from the platform or sends it by e-mail), the file must not have been modified/edited/updated by special computer programs (automatically checked by SumSub). Photographs of documents and the User must be legible and the following information must be clearly legible: the person's first and last name; date of birth and/or personal identification number, photograph and/or facial image, the person's signature, the expiry date and number of the document, the name of the issuing authority, nationality and place of birth. The document must be complete and must not be tampered. In addition to the identity document, the customer takes a photo of their face in the SumSub platform in the online mode and takes the photo with the presented identity document in their hand (a so-called selfie). Also, SubSum performs a “liveness check” to ensure, that photo of the face is made by real person in real time.
- 8.4. For identity verification purposes the User (private individual) provides identity document (passport or ID card).

## **9. TRAINING PROGRAM**

- 9.1. The Company shall implement AML/CTF training program appropriate for their size and business activities to ensure that the Company's staff which is required to have undergone AML/CTF awareness training;
- 9.2. Within the framework of the training, the Company explains to its staff the AML/CTF requirements and provide detailed information on the measures and activities the staff are expected to conduct within the framework of their responsibilities.
- 9.3. When providing the specified categories of employees with the AML/CTF training, the Company takes into consideration the knowledge and qualifications necessary for the duties, responsibilities and authorization of staff.

## **10. RECORD-KEEPING**

- 10.1. The Company shall keep records of all CDD measures, including customer identification data and documents obtained through the CDD/KYC process, policies, controls and procedures, account files and business correspondence etc.
- 10.2. The records shall be maintained for a period stipulated by law: for at least five years from the date of termination of the Business relationship in a manner, which facilitates its easy retrieval as and when required.
- 10.3. Applying the CDD measures, the Company obtains and processes the personal data of natural persons in accordance with law.

## **11. RESPONSIBILITY FOR NON-COMPLIANCE WITH THE AML POLICY AND ITS BREACHES**

- 11.1. The Company does expect compliance with applicable rules and regulations.
- 11.2. If appropriate, disciplinary punishments for non-compliance with this AML Policy and procedures and policies of the Company in the AML/CTF field may be applied.
- 11.3. Breach of AML/CTF rules and regulations may lead to criminal or administrative penalties, as well may have serious consequences – imposition of fines, reputation risk, imposition of sanctions – to the Company, its employees and Users.

## Annex 1

### List of internally prohibited jurisdictions for Talent registration

1	North Korea
2	Afghanistan
3	Iran
4	Myanmar
5	Russia
6	South Sudan
7	Sudan
8	Syria
9	Venezuela
10	Yemen
11	Zimbabwe
12	Palestine State
13	Kosovo
14	Mali
15	Nicaragua
16	Western Sahara
17	Cuba
18	Belarus
19	Central African Republic
20	Democratic Republic of the Congo
21	Iraq
22	Libya
23	Somalia
24	United States of America

## Annex 2

### The list of services that are prohibited from being provided/offered by a Talent

1. **Adult Services & Pornography** – NM Finance does not allow any exchange of adult oriented or pornographic materials and services.
2. **Fraud / Unlawful Use** – You may not use Protocol functionality for any unlawful purposes or to conduct illegal activities, such as:
  - a. Promoting prohibited or potentially dangerous goods (firearms, ammunition, drugs, and controlled substances), or encouraging others to make, use, or trade these goods;
  - b. Any level of sexual exploitation, abuse, or human trafficking;
  - c. Providing fake or misleading documents, including the creation of—or any kind of modification to—official documents such as IDs, passports, driver's licenses, bank statements, death or birth certificates, etc.;
  - d. Content which is related to glorification and/or incitement to violence, self-harm, or any other form of criminal and harmful behavior towards an individual, group, or animals;
  - e. The intention to create or promote the spread of fake news and disinformation;
  - f. Providing licensed professional services, e.g., legal counsel, financial or tax advice, etc.;
  - g. Attempts to hack or crack any system (accounts, profiles, networks, etc.) with the intent to obtain unauthorized access to sensitive personal and/or financial information of individuals, entities, or governmental institutions;
  - h. Creating or contributing to any information security hazard for individuals, entities, governmental institutions (DDOS attacks, doxxing, impersonation, distribution of malware, phishing and other hacking techniques, etc.).
3. **Misleading or Deceptive Services** (including but not limited to misrepresentation of qualifications or impersonation).
4. Services that involve **sharing personal information** of third parties.
5. Services which infringe on copyrights, trademarks, patents, or any other **intellectual property rights** of third parties.

Failure to adhere to these prohibitions may result in the immediate termination of the Talent Profile. The Company reserves the right to investigate and take appropriate action against any Talent found to be in violation of these prohibitions, including reporting illegal activities to relevant authorities.