DMA LINK LIMITED

Due Diligence, Anti-money Laundering and Countering the Financing of Terrorism Policy

Revision 4.0

Document Particulars. Refer to the table below.

Document Title	Due Diligence, Anti-money Laundering and Countering the Financing of Terrorism Policy		
Documents Code	DDIL001		
Owner(s)	Board of Directors		
Administrator(s)	Compliance Officer ("CO") and Money Laundering Reporting Officer ("MLRO")		
Created Date (Original)	1 February 2021		
Department	Management		
Users	All directors, employees, agents, contractors, consultants		
Revision	4.0		
Revision Date	11 August 2023		
Amendments By	Ashwind Soonarane (COO)	Signature	

Purpose and scope. This document establishes policies and guidelines pursuant to legal and regulatory obligations applying to the Company in respect of customer due-diligence, anti-money laundering and the countering of financing of terrorism. It further covers the reporting of suspected or actual cases in view of preventing, wherever possible, the Company or its people from being exposed to money laundering, proceeds of crime, and/or the financing of terrorism.

Prerequisites. Staff Manual and Money Laundering Training (in-house)

Summary of changes. The name of the document has been amended from "Due-Diligence Policy". Further, sections - Disclosure procedure, Due-diligence process, Unauthorised activities, Whistleblowing – and Appendices A and B have been amended and/or added to the document.

Prior documents deprecated. Due Diligence Policy (version 2.0)

Document Approval: This document is reviewed by the Administrator(s) and approved by the Owner(s)

Title	Name	Date
Chairman of the Board of Directors	Manu Choudhary	11 August 2023
Compliance Officer	Chris Park	11 August 2023
Money Laundering Reporting Officer	Chris Park	11 August 2023

DMALINK

Table of Contents

1 Introduction

DMALINK (the "Company") prohibits the use of proceeds of crime and actively pursues the prevention of money laundering, including any activity that facilitates money laundering or the funding of terrorist or criminal activities. It is especially noted that a relatively low level of funds may be required for significant acts to be carried out by offenders.

The Company has implemented a risk-based approach in preventing, detecting and reporting transactions reasonably deemed to originate from or result in the proceeds of crime, money laundering, corruption, and terrorist financing. All risk assessments, verifications and other relevant efforts will be documented and records will be retained for at least five (5) years or in accordance with English Law and applicable rules and regulations. The Company shall report and provide all available information relating to such transaction or matter to the appropriate law enforcement or regulatory agencies without unreasonable delay.

The Company shall ensure that all business units including its affiliates, subsidiaries, and any other entity which exercises reasonable control over, or is under the reasonable control of, DMALINK comply with this Policy and apply best efforts against money laundering and other criminal activities pursuant to this Policy. Any contact by law enforcement or regulatory agencies related to the Policy or in connection with any activity shall be directed to the CO and MLRO as set out in Appendix A.

This policy ("Policy") applies to all Relevant Persons of the Company. It covers aspects of Anti-Money Laundering (AML), Countering-Terrorist Financing (CTF), Know-Your-Customer (KYC) rules such that the Relevant Persons may identify and report previous, present, and potentially future exposure (included any suspected exposure) to any illegal practice.

2 Definitions

"**Affiliate**" means, with respect to any Person, any other Person who directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. The term "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract or otherwise, and the terms "controlled" and "controlling" shall have meanings correlative thereto.

"**Applicable Jurisdiction**" means the United Kingdom, United States of America, the European Union, and including any other jurisdiction where the Company (including any Affiliate) may be regulated that becomes relevant in respect of any business relationship between the DMALINK and any Person.

"**Business Day**" means any day, except for Saturday, Sunday, and any bank holiday, where commercial banks are open in London, United Kingdom for the normal course of business.

"**Person**" means an individual, partnership, limited partnership, corporation, limited liability company, joint stock company, unincorporated organization or association, trust or joint venture, or a Governmental Authority or political subdivision thereof.

"**Platform**" means any Electronic Communication Network (ECN) or trading platform operated by the Company.

"**Relevant Person**" means any director, officer, employee, partner, agent, contractor, appointed representative[1] (as defined by the FCA, and where applicable a tied agent[2]) of the Company.

3 What is money laundering

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

Criminals generally go through a three-stage process, as defined below, to convert criminally derived proceeds or "dirty" assets into any "clean" assets so as to hide and change their true identity. Once legitimized as "clean" assets, they are able to circulate freely within the financial system.

Placement stage. The proceeds of crime or "dirty" asset is placed directly into the financial system. For example, cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions.

Layering stage. The proceeds of crime are moved through a series of financial transactions, making it harder to establish their origin.

Integration stage. The money launderer creates a legitimate explanation for the source of the funds allowing them to be retained, invested into the legitimate economy or to acquire assets

3.1 Acts of money laundering

A range of activities, considered offences under law, in relation to money laundering are covered in:

(a) The Proceeds of Crime Act 2002[3] (as amended by the Crime and Courts Act 2013, Serious Crime Act 2015 and the Criminal Finances Act 2017[4])
(b) The Terrorism Act 2000[5] (as amended by the Criminal Finances Act 2017)
(c) The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer)[6] Regulations 2017 (as amended by the Money Laundering and Terrorist Financing (amendment) Regulations 2019).

The most common examples of the act of money laundering are as follows:

(a) Concealing, disguising, converting or transferring criminal property or removing it from the UK;
(b) Entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person;
(c) Acquiring, using or possessing criminal property;

[1] https://www.handbook.fca.org.uk/handbook/glossary/G1659.html
[2] https://www.handbook.fca.org.uk/handbook/glossary/G1983.html
[3] https://www.legislation.gov.uk/ukpga/2002/29/contents
[4] https://www.legislation.gov.uk/ukpga/2017/22/contents
[5] https://www.legislation.gov.uk/ukpga/2000/11/contents
[6] https://www.legislation.gov.uk/uksi/2017/692/contents

(d) Failure to disclose knowledge or suspicion of another person(s) involvement in money laundering; and
(e) Tipping off or making a disclosure which is likely to prejudice an investigation being carried out by a law enforcing authority, knowing that such an investigation is in motion.

Please be aware that any Relevant Person may commit an offence under the money laundering provisions if such person suspects money laundering but fails to take any action or becomes involved with it in some way. Disciplinary action may result as a failure of any Relevant Person to comply with this procedure.

Refer to Appendix B for additional information.

4 What is the financing of terrorism

The financing of terrorism relates to any form of support being provided in relation to terrorism or those who encourage, plan or engage in terrorism.

It must be noted that funds used in support of terrorism can originate from legitimate sources (e.g., an individual's salary) or illegitimate sources (e.g., proceeds of crimes such as selling of counterfeit goods, fraud or drug trafficking).

The use of proceeds of crime in the financing of terrorism will generally be disguised such that their illegitimate origins will appear to come from legitimate activities, as described in Paragraph 3. However, in the vast majority of cases, people engaged in the financing of terrorism will disguise the intended use of any proceeds.

Terrorist financing often involves a complex series of transactions, generally considered as representing three separate phases and this could be sourced through various means for example through seeking donations, carrying out criminal acts and from genuine charities, as illustrated below.

Collection. Funds are often acquired through seeking donations, carrying out criminal acts or diverting funds from genuine charities.

Transmission. Funds are pooled and transferred to a terrorist or terrorist group.

Use. Funds are used to finance terrorist acts, training, propaganda, amongst others.

5 Consequences of money laundering and terrorist financing

Money laundering and the financing of terrorism can have serious negative consequences for the economy, national security, and society in general. Failing to identify and take appropriate measures against the foregoing may constitute an offence under law and have significant consequences on the Company and its continued operations.

Reputational damage. By being associated with money laundering and terrorist financing, the Company's brand and general image will be damaged such that its relationships with existing and future clients or

providers may suffer.

Regulatory sanction. The Company may face serious consequences from regulatory authorities overseeing its business. Regulatory authorities may impose fines or other sanctions on the Company that may not be overcome.

Business continuity. Key providers enabling the Company's business may off-board the Company leading to a complete stop of business operations, even if arising from legitimate counterparties.

Company and people. The Company including any Relevant Person, failing in their duty to comply with law and regulations, may be exposed to criminal charges.

6 Key persons and responsibilities

6.1 Compliance Officer (CO)

In respect of regulated activities being carried out by the Company, DMALINK is required to appoint a CO. Please bear in mind that the CO must not be involved in the performance of the services or activities the he/she monitors.

The responsibilities of the CO include:

(a) regular monitoring and assessment of the adequacy as well as effectiveness of Company measures, policies and procedures; and
(b) advising and assisting Relevant Persons responsible for, or involved in, the carrying out of any regulated activity.

6.2 Money Laundering Reporting Officer (MLRO)

Pursuant to English law, the Company is required to:

(a) appoint a MLRO, and in the absence of the MLRO designate a person, to receive disclosures from employees of money laundering activity (their own or in respect of any other person); and
(b) implement adequate procedures to enable the reporting (including on suspicion) of money laundering; and
(c) maintain client identification procedures in certain circumstances; and
(d) maintain record keeping procedures.

The responsibilities of the MLRO include:

(a) receiving disclosures about money laundering activity; and
(b) ensuring that the Company complies with relevant laws and regulations; and
(c) providing training to Relevant Persons in respect of company policies and procedures relating to money laundering.

7 Due diligence process

7.1 Know-Your-Customer (KYC)

The Company will ensure that adequate due diligence has been successfully completed prior to entering into any business relationship or transaction (the "Transaction") with any counterparty, provided that the Transaction involves (a) a non-regulated or regulated product on the Company's Platform; or (b) a net cash or other payment of at least €10,000 or equivalent.

The Company will provide notice to such counterparty that it is requesting information pursuant to Appendix C from them to verify their identities (including the identity of any ultimately beneficiary where relevant) as required by English law.

The Company will record any verification carried out in respect of such person's identity and overall standing, including comparing Relevant Individual identification information against international databases such as WorldCheck, Kroll, CreditSafe, Chainalysis and/or any other appropriate systems at the sole discretion of the Company. Further, the Company will verify sanctions that may be in effect in respect of such counterparty.

7.2 Politically Exposed Person (PEP)

A PEP is defined as a person entrusted with prominent public functions and include (a) heads of state, heads of government, ministers and deputy or assistant ministers; and (b) members of parliament or of similar local or regional or federal legislative bodies; and (c) members of the governing bodies of political parties; and (d) judges of supreme courts, constitutional courts or judges of any judicial body whose decision is not subject to further appeal except in exceptional circumstances; and (d) members of courts of auditors; and (e) members of the boards of central banks; and (f) ambassadors, 'chargés d'affaires' and high-ranking officers in the armed forces; and (g) members of the administrative, management or supervisory bodies of State-owned enterprises; and (h) directors, deputy directors and members of the board or equivalent function of an international public organization.

The definition of PEP includes (a) his/her family members such as spouse, father, mother, sons, daughters, sisters and brothers; and (b) any person known to be a close associate where the term "close associate" means an employee or partner of the PEP, or a firm represented or owned by the PEP, or any person with family or other links to the PEP.

PEPs are required to be subject to enhanced scrutiny by firms subject to the English law.

The Company will not automatically decline to establish or suspend any existing business relationship with any person upon being classified as a PEP. However, the Company must carry out a risk assessment in respect of money laundering, terrorist financing associated, corruption or bribery (including the proceeds thereof) associated with the relationship being established, or existing with, the PEP. The Company will make use of publicly available information that is reasonably at its disposal in identifying PEPs, including their family members or known close associates. The Company may further carry out verifications in respect of PEPs against international databases mentioned in Paragraph 7.1.

A PEP shall retain his/her classification and be subject to enhanced diligence for a minimum period of 12 months after that person ceases to be a PEP.

7.3 Sanctions in effect

Sanctions are measures taken by one or more countries against another in response to perceived violations of international law, human rights abuses, aggression towards other nations, or other objectionable behaviour. The aim of sanctions is to discourage or penalize certain actions or policies and encourage a change in behaviour or compliance with specific demands set forth by the sanctioning entity. Similarly, individuals and organisations engaging in illegal activities may end up on sanctions lists or watchlists. Such activities include:

(a) money laundering
(b) terrorism and terrorist financing
(c) drug trafficking
(d) human-rights violations
(e) arms proliferation
(f) violation of international treaties

As part of its due-diligence procedures, the Company will verify whether any entity with which it intends to enter into Transaction (as defined in paragraph 7.1) is subject to any sanction, within the Applicable Jurisdiction (refer to Definitions), in respect of such Transaction. The Company may refer to sanctions list of the UK[7], US[8], EU[9], as well as other relevant lists for its verifications.

The Company will not automatically decline to establish or suspend any new or existing business relationship with any entity subject to sanctions. However, the Company must carry out a risk assessment, in respect of Applicable Jurisdictions, evaluating the type of activity being sanctioned and the impact of effecting Transaction. The Company may, at its sole and absolute discretion, include designated entities on its watch-list to ensure ongoing compliance with law through regular risk assessments and verifications. For the avoidance of doubt, the Company will suspend any Transaction, upon becoming aware or as established through this policy by the Company, that is subject to sanctions with immediate effect.

7.4 Reliance on third-parties

Reliance on third-parties means the process whereby DMALINK relies on a regulated third-party financial institution that is subject to monitoring, supervision, reporting and other obligations in respect of CDD, AML, CFT under the Applicable Jurisdiction to obtain information relating to and/or to undertake any Transaction (as defined in paragraph 7.1) with the Company's clients.

In respect of any Person, the Company may at its sole and absolute discretion may deem that its CDD, AML, CFT obligations shall be fulfilled by a regulated third-party financial institution having onboarded such Person as a client for the purpose of transacting on the Platform and which is subject to the terms of a legally binding agreement with Company to perform any of the following services in respect of the

[7] https://www.gov.uk/government/publications/the-uk-sanctions-list
[8] https://ofac.treasury.gov/sanctions-programs-and-country-information
[9] https://www.sanctionsmap.eu/#/main

Platform:

(a) Prime brokerage and/or credit intermediation; or
(b) Central clearing agent or settlement agent in respect of Platform transactions; or
(c) Custodian of client assets; or
(d) Acting as a bank, the delivery of any security interest by such client to the Company.

7.5 Verifying information

Based on the risk, and to the extent reasonable and practicable, DMALINK will ensure that it has a reasonable belief of the true identity of any Relevant Individual. In verifying a Relevant Individual's identity, DMALINK shall review photo identification. DMALINK shall not attempt to determine whether the document that the Relevant Individual has provided for identification has been validly issued. For verification purposes, DMALINK shall rely on a government-issued identification to establish a Relevant Individual's identity. DMALINK, however, will analyse the information provided to determine if there are any logical inconsistencies in the information obtained. DMALINK will document its verification, including all identifying information provided by the Relevant Individual, the methods used and results of the verification.

7.6 Monitoring and reporting

Transaction based monitoring shall occur within the appropriate business units of DMALINK. Monitoring of specific transactions shall include but not limited to transactions aggregating €10,000 or more (irrespective of whether such transaction is completed in a single event or split across several events), and those with respect to which DMALINK has a reason to suspect suspicious activity. All reports shall be documented. Note that any payment arising from adequate consideration from a provider of any service shall not constitute a transaction that qualifies for monitoring, including when net transactions exceed the above-stated amount.

7.7 Suspicious activity

Any sign, deemed, suspected or foreseen, of suspicious activity or irregularity in connection with AML, CTF, KYC will commonly be referred to as "red flags". If a red flag is detected, additional due diligence will be performed before proceeding with any transaction. If a reasonable explanation, with relevant supporting documents where the context so requires as evidence, is not determined, the suspicious activity shall be reported to the MLRO, and to the members of the board of directors of DMALINK at the earliest opportunity.

7.8 Investigation

Upon notification to directors of DMALINK an investigation will be commenced to determine if a report should be made to appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrant, a recommendation will be made to the directors of DMALINK to file a blocked assets reports with the appropriate law enforcement or regulatory agency. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any party disclose or discuss any AML, CTF, KYC concern, investigation, notice or report filing with the person or persons subject of such, or any other person.

7.9 Ongoing business relationships

It is the policy of DMALINK to keep due diligence in connection with Relevant Individuals up to date. DMALINK shall further ensure that an appropriate level of on-going monitoring for existing business relationships is in place.

8 Unauthorised activities

8.1 Cash Payments

Cash payment exceeding £1,000 in connection with the Company must not be accepted or made by Relevant Person without the prior approval of, and guidance from, the MLRO. Each Relevant Person will:

(a) put the cash transaction on hold prior to the transaction taking place; and
(b) report details of the cash transaction to the MLRO; and
(c) assist the MLRO by providing any additional information that may be required in order to perform relevant checks; and
(d) abide by the guidance received from the MLRO in respect of the transaction.

8.2 Receiving and giving gifts

In respect of any Relevant Person, the receiving or giving of gifts, irrespective of value, is not authorised to the extent that such gift is being made in return for (a) any implied or disclosed favour, including but not limited to any action or inaction, to be undertaken by the receiving party for the benefit of the giving party (or any person associated with such party including the Company); and (b) any payment to be given to the giving party.

For the avoidance of doubt, the term "gift" includes any monetary fund (fiat or digital currency), item or object, payment in respect of any service (e.g., flights, hotels, and other), the delivery of any form of benefit (immediate or future) to the receiving party.

The prior approval of the Company is required in the event that any gift (including a series of gifts being made over any 12 months period), having a total estimated market value exceeding £50, is being given or received provided that such exchange is made without any further expectation, e.g., over the Christmas period or other as the case may be.

Failure to abide by this Procedure may result in disciplinary procedure.

9 AML/CFT disclosure procedure

When any person has reasonable grounds to suspect that any activity may be connected to AML or CTF (or where any activity is simply suspicious), the matter must be reported to the MLRO. Likewise, any activity undertaken without completing due-diligence (such as KYC) must be reported to the MLRO.

Note that disclosures must be made to the MLRO even if the person making any disclosure does not have actual evidence of activities involving money laundering or the proceeds of crime.

If you are unsure as to whether any activity, involving you or any person associated with the Company, may constitute or be deemed a breach of AML, CFT, or KYC rules, please contact the MLRO of the company (refer to Appendix A) as soon as possible, and to the extent under your control, prior to engaging in such activity.

Notwithstanding the foregoing, where any disclosure is to be made against or involves the MLRO in some way, such disclosure must be made to one of the following officers of the Company provided that no connection can be established in the disclosure to the person receiving the disclosure:

(a) Chief Executive Officer
(b) Chief Operations Officer
(c) Chief Financial Officer

In such cases, the relevant officer will be responsible (a) for carrying out an independent verification of the MLRO's potential involvement in any disclosure; and (b) fully investigate the matter being raised by any disclosure; and (c) take appropriate corrective and preventive measures.

10 Whistleblowing

Particular attention must be paid to situations where there is any exchange of funds, especially in respect of:

(a) unfamiliar or new sources and/or relationships (e.g., client or any other person)
(b) significant amounts on a one-off basis and/or gifts

Evidence of the identity of the prospective client (or any other person) should be obtained before proceeding. Any Relevant Person involved in a transaction of this kind should ensure that the person has provided satisfactory proof of identity, proof of address, and any other document in accordance with the Due-Diligence Policy of the Company.

11 Reporting to the Money Laundering Reporting Officer

If any person becomes concerned that their involvement in any matter may amount to a prohibited act under the legislation, must disclose this promptly to the MLRO.

Time is of essence in respect to any disclosure. Therefore, disclosures must be at the earliest opportunity of the information coming to your attention. Failure to take prompt action or any unreasonable delay in effecting any disclosure may result in risk of prosecution.

Each Relevant Person must follow any subsequent directions from the MLRO. Once a matter is referred to the MLRO:

(a) the Relevant Person must not make any further enquiries into, or take any further steps in, such matter without the prior approval of the MLRO; and
(b) the Relevant Person must not disclose or otherwise indicate their suspicions to any other person,

irrespective of whether such person may be connected with the matter or otherwise suspected of any illegal activity or of failing any obligation under this Policy

(c) the Relevant Person must not disclose or otherwise record (or keep a note) on any media accessible to any other person that a report has been made to the MLRO

For the avoidance of doubt, if any payment exceeding £1,000 is due to any person connected with a matter reported to the MLRO, such payment shall be not be made without the prior approval of the MLRO, CO, and the Board of Directors.

12 Consideration of the disclosure by the Money Laundering Reporting Officer

The MLRO shall:

(a) promptly evaluate any disclosure to determine whether it should be reported to the National Crime Agency (NCA) or other competent regulatory body in respect of the Applicable Jurisdiction; and

(b) if they so determine, promptly report the matter to the relevant regulatory body in accordance with such regulator's procedures, including via any standard report form that may be prescribed; and

(c) notify the Board of Directors of any report submitted to the regulator; and

(d) retain all disclosure reports referred to the MLRO, including all reports made to the regulator, for a minimum of five years, or pursuant to the Company's data policy if exceeding 5 years, in a confidential file made for that purpose; and

(e) record any action taken on the Money Laundering Disclosure Form (Appendix D).

The MLRO will commit a criminal offence if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering and they do not disclose this as soon as practicable to the regulator.

13 Record Keeping

The CO and MLRO shall have an obligation to keep a record of all data, reporting, referrals made to then, including any information in respect of investigations carried out. This further includes data that may be obtained from public sources of information, disclosed to the company by any third-party, including third-party systems or databases such as WorldCheck, Kroll, CreditSafe, Chainalysis. Actions taken, and where relevant in the event that any action was omitted, must be documented. It is worth noting that the precise nature of these records is not specified in law. Therefore, appropriate steps must be taken to ensure, at a minimum requirement, that sufficient information is kept to perform, or permit, an audit trail or further investigation at any point in time.

14 Guidance and Training

DMALINK will at all times employ a Relevant Person who possess the necessary skills, knowledge and expertise to carry out their function effectively. In addition, the Company will take relevant steps to ensure that:

(a) each Relevant Person is informed of the requirements and obligations applying to the Company within the jurisdictions it operates;
(b) each Relevant Person is competent in carrying out the functions applying to such Relevant Person pursuant to applicable law;
(c) each Relevant Person is provided with adequate training

15 Policy review

This Due Diligence, Anti-money Laundering and Countering the Financing of Terrorism Policy will be reviewed by the Money Laundering Reporting Officer and Compliance Officer on a yearly basis, or on an ad-hoc basis at the sole discretion of the Company, to ensure it continues to comply with applicable law and implements best industry practices in respect of customer due-diligence, anti-money laundering and the countering of financing of terrorism.

APPENDIX A

Notice to DMALINK

Notices under or in connection with this Policy must be made to the Compliance Officer and/or the Money Laundering Reporting Officer.

Compliance Officer

The Compliance Officer
DMA LINK LIMITED
71-75 Shelton Street
Covent Garden
London
ENGLAND WC2H 9JQ

Email: compliance@dmalink.com

Money Laundering Reporting Officer (the "MLRO")

The Money Laundering Reporting Officer
DMA LINK LIMITED
71-75 Shelton Street
Covent Garden
London
ENGLAND WC2H 9JQ

Email: MLRO@dmalink.com

Notices must be made in writing and (a) sent by high priority registered post; or (b) electronically at the above-stated e-mail address. Notices will be deemed to have been given (a) on the next Business Day that such notice is received by DMALINK if sent by high priority registered post; and (b) on the next Business Day such notice is received by DMALINK if sent by electronically.

APPENDIX B
Offences Table

Applicable Law	Offence & Definition[10]
S327 Proceeds of Crime Act 2002	Money Laundering Offence: Concealing Criminal Property A person commits an offence if they conceal, disguise, convert or transfer criminal property or if they remove criminal property from England, Wales, Scotland or Northern Ireland. This is punishable by a maximum term of imprisonment of 14 years at the Crown Court and an unlimited fine. At the Magistrates Court it is 6 months and £5,000 fine.
S328 Proceeds of Crime Act 2002	Money Laundering Offence: Arrangements This offence requires a person to become actively involved in some arrangement which helps someone else to get, keep, use or control the proceeds of a crime. The punishment is as for S327.
S329 Proceeds of Crime Act 2002	Money Laundering Offence: Acquisition, Use and Possession This offence is committed by anyone that has criminal proceeds in their possession provided they know or suspect that it represents the proceeds of a crime unless they paid 'adequate consideration' for it. Someone who pays less than the open market value is therefore guilty of the offence but someone who pays the full retail price, despite knowing or suspecting they are stolen goods is not guilty. The punishment is as for S327.
S330 Proceeds of Crime Act 2002	Failure to Disclose Offence: Regulated Sector This offence is committed by an employee of a business in the regulated sector who has knowledge or suspicion of another person's involvement in money laundering and does not make a report through the appropriate channels. Negligence is not a defence as the employee will be tried upon what they should have known given their experience, knowledge and training. This is punishable by a maximum term of imprisonment of 5 years and/or a fine.
S331 Proceeds of Crime Act 2002	Failure to Disclose Offence: Nominated Officers in the Regulated Sector This offence is committed by a nominated officer (MLRO) of a business in the regulated sector who has knowledge or suspicion of another person's involvement in money laundering and does not make a report through the appropriate channels without an acceptable excuse under the legislation. Negligence is not a defence as the nominated officer will be tried upon what they should have known given their experience, knowledge and training. This is punishable by a maximum term of imprisonment of 5 years and/or a fine.

[10] Imprisonment term and/or fine in respect of any offence is subject to the applicable law, as amended from time to time by competent bodies in the UK

APPENDIX C

Due-diligence document checklist

Original copies, or a notarized copy, of the requested documents must be provided unless otherwise specified by, or agreed with, the Company.

In regards to a natural person (private individual)

(a) Proof of identity: passport and/or driving licence
(b) Proof of residential address (two independent source): utility bill, bank statement
(c) Declaration of source of funds

In regards to a legal person (e.g., a company)

(a) Proof of identify:
    - certificate of incorporation
    - memorandum and articles of association (or comparable documents)
    - Legal Entity Identifier (LEI), if available
(b) Proof of trading address: utility bill, tenancy agreement, bank statement
(c) Nature of business: company classification
(d) Declaration of source of funds
(e) Authorised signatory list / Certificate of Incumbency
(f) CDD, AML, and CFT policies/procedures

Additional information is required in respect of any person accessing the Platform and entering into transactions with DMALINK on a principal-to-principal basis:

(a) Most recent audited accounts

Additional information is required in respect of directors/trustees, and ultimate beneficiaries (where the ultimate beneficiary is a natural person)

(a) Director/trustee/other:
    - Proof of identify: passport and/or driving licence Identification documents of at least 1 director/trustee
(b) Ultimate beneficiary (in respect of shareholders with at least 20% ownership or control):
    - Proof of identity: passport and/or driving licence
    - Proof of residential address: utility bill, bank statement
    - Declaration of source of funds

APPENDIX D

Money-Laundering Disclosure Form

To: Money Laundering Reporting Officer (MLRO)		
Name		
Title		
Tel number		
Email address		
Nature, value and timing of activity involved Full time employee and director of the business		
Transaction suspended	Yes ☐	No ☐
Urgent	Yes ☐	No ☐
If urgent, please state by when (date) such transaction had to be normally effected and provide additional details where relevant:		
Details of suspected offence:		
Names and contact details of person(s) involved		
Details of suspected offence:		
Nature of suspicions regarding the activity:		
Has any investigation been undertaken (as far as you are aware)?	Yes ☐	No ☐
If yes, please give details below:		
Are there any evidence confirming or in connection with the suspicious activity?	Yes ☐	No ☐
If yes, please give details below (or attach any supporting document to this form):		

Have you discussed your suspicions with anyone?	Yes ☐	No ☐
If yes, please specify below and explain why the discussion was necessary:		
Please set out below any other information you feel is relevant:		
Signed:		
Dated:		
Details of verifications/MLRO notes (attach supporting documents to this form):		
Signed:		
Dated:		