Anti-Money Laundering and Counter-Terrorism Financing Policy

1. Introduction

This Anti-Money Laundering and Counter-Terrorism Policy (the **"Policy"**) outlines the approach of Key to Markets Limited, a company incorporated as a Private limited company in England and Wales under Companies House number 07276568 and authorised and regulated in the United Kingdom by the Financial Conduct Authority under Firm Reference number 527809, whose registered address is at Vicarage House – 58-60, Kensington Church Street, London, W8 4DB (the **"Company"**), to preventing and detecting money laundering and terrorist financing. In developing this policy, the Company has considered all current anti-money laundering and counter terrorist financing obligations required by the United Kingdom law, as well as by the industry best practices. This Policy has been created utilising guidance issued by the Financial Conduct Authority, Her Majesty's Revenue & Customs (HMRC) and the Joint Anti-Money Laundering Steering Group (JMLSG).

The Company fully acknowledges that its products and services are at risk from individuals or groups seeking to launder criminal proceeds or facilitate funds designated for the financing of terrorism. As such, the Company is committed to fostering and promoting a compliance culture, which underpins the importance of preventing money laundering and terrorist financing.

The Company recognises it has a statutory duty under the UK law to prevent the facilitation of its services for money laundering and terrorist financing purposes. Subsequently, the Company pledges to allocate sufficient resources to its internal controls, monitoring system, human resources and staff training to prevent financial crime.

1.1. Scope

All Company's employees, directors, officers and associated agents are required to comply with this Policy. Failure to do so may result in disciplinary action.

1.2. Definitions

The following abbreviations and terms shall have the following meanings:

AML/CTF – anti-money laundering and counter-terrorism financing;

Applicable Regulation –

- Proceeds of Crime Act 2002 (POCA), as amended by the:
    - Serious Organised Crime and Police Act 2005 (SOCPA) and the
    - Proceeds of Crime Act (Amendment) Regulations 2007;
- Terrorism Act 2000, as amended by the:
    - Anti-terrorism, Crime and Security Act 2001 and the
    - Terrorism Act (Amendment) Regulations 2007;
- Terrorism Act 2006;
- Counter-terrorism Act 2008, Schedule 7;
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("**MLR"**), as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019;
- HM Treasury Sanctions Notices and Guidance and News Releases;
- FCA Handbook;

- Joint Money Laundering Steering Group (JMLSG) Guidelines for the UK Financial Sector on the prevention of money laundering/combating terrorist financing;
- 4MLD.

Board – board of directors of the Company;

FATF - Financial Action Task Force;

FCA– Financial Conduct Authority;

4MLD – Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;

HTM – Her Majesty's Treasury;

Lists of Terrorists – the lists of persons who are believed to be involved in terrorist activity;

MLRO - money laundering reporting officer;

NCA - National Crime Agency;

NCCTs – Non-Cooperative Countries or Territories, which FATF judges to be non-cooperative in the global fight against money-laundering and terrorist financing; the list of NCCTs can be found at: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

OFSI - Office of Financial Sanctions Implementation;

PEP – a natural person, who is or has been entrusted with a prominent public function such as government official, senior executive of government corporation, politician, political party official, etc., their family member and close associates;

Procedures - Client Due Diligence Procedures, a written policy summarising the measures the Company takes to effectively mitigate and manage its risk of money laundering and terrorist financing;

Sanction Lists – any official lists of Sanctioned persons as well as the Lists of Terrorists;

Sanctioned person – a person, who is subject to financial sanctions and who is included in the list of sanctioned parties maintained by the HMT (**"HTM list"**);

Screening Software – LexisNexis Platform or any other risk management solution aimed at identifying risks, which includes the Sanction Lists issued by the UK, EU and other international sanctioning bodies;

Suspicious Activity Report – a report about a Suspicious Transaction.

For the purpose of this Policy, the term "**person**" shall include a reference to any natural person or a legal person.

For the purpose of this Policy, the term "**legal person**" includes a reference to bodies corporate, partnerships, associations or any other organisation or arrangement (whether or not having a separate legal personality).

Words importing the singular number include the plural and vice versa and words importing the masculine gender include the feminine and neuter genders.

1.3. Objectives

The objectives of this Policy are to:

- Emphasise the Company's stringent commitment to preventing itself from being used as a conduit to deposit, conceal and transfer criminal proceeds or funds intended for orchestrating terrorism;
- Summarise the main procedures, systems, and controls the Company has implemented to prevent and detect money laundering and terrorist financing;
- Clearly outline the responsibilities of the Company's senior management, MLRO and other key individuals in relation to the Company's AML/CTF strategy;
- Explain the most up-to-date money laundering and terrorist financing risks that the Company is vulnerable to and how the Company intends to counteract these risks;
- Confirm that the Company will take steps to monitor compliance by all staff with this Policy.

2. What is Money Laundering?

The Company views money laundering to be the process by which illegally gained proceeds or funds are cleaned and sanitised to disguise their illicit origins.

Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. It also includes money, however come by, which is used to fund terrorism.

Money laundering activity can include:

- Acquiring, using or possessing criminal property;
- Handling the proceeds of crimes such as theft, fraud and tax evasion;
- Being knowingly involved in any way with criminal property;
- Entering into arrangements to facilitate laundering criminal property.

The money laundering process traditionally follows three stages:

Placement

The placement stage represents the initial entry of proceeds derived from an illegal activity into the financial system. It is during the placement stage when criminal transactions are most vulnerable to detection.

Layering

Layering is the most complex stage of the process, where criminals aim to separate the illegal proceeds from their illicit origin. This is traditionally done via several complex transactions within the international financial systems. It is common for criminals at this stage to transfer funds electronically between jurisdictions and invest them into advanced financial products or overseas markets. This is done repeatedly to obscure the audit trail and decreases the probability of law enforcement authorities tracing the proceeds to their original crime.

Integration

It is at this final stage where the money is returned to the criminal as "clean" funds as they appear to come from a legitimate source. Having been "placed" as cash and "layered" through several complex financial transactions, the criminal proceeds are now "integrated" into the financial system and can now be used for any purpose.

3. What is Terrorist Financing?

The Company views terrorist financing to be the use of funds, or the making available of funds, for the purposes of terrorism. This constitutes the funds that both individuals and organisations contribute towards financing terrorist activities or terrorist organisations.

The source of terrorist financing can take many forms, including:

- Self-financing from individuals, including but not limited to income from employment, savings, borrowed money from families or friends and bank loans;
- Funds raised by legitimate charities affiliated to or sympathetic to terrorist ideology;
- States directly or indirectly sponsoring terrorist groups.

The Company is committed to ensuring that:

- Our clients are not terrorist organisations themselves;
- We are not providing the means through which terrorist organisations can be funded (i.e. by providing loans and other services to individuals who intend to finance terrorism).

4. Responsibilities of MLRO and Senior Management

The Company clearly defines the roles and responsibilities of all individuals with oversight of the Company's AML/CTF strategy and responsibility for the Company's compliance with all AML/CTF requirements.

4.1 MLRO

The Company appointed a senior officer, who is judged by the Board to be fit and proper to hold the role, as the Company's MLRO. The MLRO assumes responsibility for oversight of the Company's AML/CTF strategy and its compliance with the Applicable Regulation with regards to systems and controls against money laundering and terrorism financing.

The MLRO:

- Receives and investigates Suspicious Activity Reports;
- Reports on behalf of the Company to the NCA, OFSI or HMT's Asset Freezing Unit;
- Ensures the suitability of the content of the AML/CTF training and the subsequent roll-out of the training to all staff and advisers across the Company;
- Reports at least annually to the Board on the operation and effectiveness of the Company's AML/CTF systems and controls;
- Monitors day-to-day operation of the Company's AML/CTF policies and responds promptly to any reasonable requests for information made by the FCA or law enforcement bodies;
- Approves and conducts the risk-assessment of new or amended products/jurisdictions/sales channels;
- Approves business relationships which the Company wishes to enter into or continue, and where the client poses a high risk of money laundering or terrorism financing (for example, client is a PEP or a Sanctioned person or resides in or trades with a jurisdiction with weak measures to combat money laundering and terrorist financing, which is publicly identified by FATF as a high risk or non-cooperative);

- Establishes and maintains policies, controls, and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in any risk assessment;
- Makes sure that all AML/CTF policies, controls and procedures are up-to-date and compliant with the Applicable Regulation.

The report, which the MLRO submits to the Board, must include the following:

- Review of the effectiveness of the Company's AML/CTF systems and controls, with appropriate recommendations for improvement in the management of risks and priorities, including resources;
- Detail those within the Company responsible for AML/CTF systems and controls;
- Concluding actions and the remedial progress in response to these;
- The number of internal SARs.

The Board will give these reports due consideration and take necessary actions to remedy any deficiencies identified by the report.

The policies, procedures and controls that the Company has in place are regularly amended and enhanced in accordance with updates to the Applicable Regulation and industry's best practice. The Company's systems and controls also change to counteract the risks identified in the regular risk assessments. Subsequently, the Company has systems in place to monitor staff compliance with the Company's policies, procedures and controls.

4.2 Senior Management

The Company's senior management takes active part in implementing and monitoring the Company's AML/CTF strategy. Particularly, the senior management:

- Ensures that the Company's AML/CTF policies, procedures, and controls are appropriately designed and implemented to reduce the Company's vulnerability to money laundering and terrorist financing;
- Is fully engaged in the decision-making process regarding the firm's AML/CTF strategy and takes ownership of their risk-based approach;
- Takes appropriate steps to identify and assess the risks of money laundering and terrorist financing to which the Company is subject;
- Ensures that the Company fulfills its obligations under the Applicable Regulation.

4.3 Employees

All Company employees are trained to identify and report suspicious activity. They are also given regular training on their obligations under the Applicable Regulation.

5. Regulatory Responsibility

As a holder of FCA license, the Company is fully aware of the regulatory framework relating to AML/CTF and carries out its activity in compliance with the Applicable Regulation. The Company also provides regular training to its employees, agents, and subsidiaries to ensure they have sufficient knowledge of the UK's regulatory framework.

6. Offences

The Applicable Regulation outlines multiple money laundering and terrorist financing offences, which the Company is committed to avoid. The key offences under the Applicable Regulation are as follows:

- **Concealing (subject to a maximum 14-year jail term and/or a fine).** It is an offence to help conceal, disguise, convert, transfer or remove funds from the UK if you know, should have known, suspect or should have suspected that the funds were the proceeds of criminal conduct;
- **Arrangements (subject to a maximum 14-year jail term and/or a fine).** It is an offence to enter into or become concerned with an arrangement if you know, should have known, suspect or should have suspected that the arrangement facilitates the acquisition, retention, use or control of criminal property;
- **Acquisition, use, and possession of funds (subject to a maximum 14-year jail term and/or a fine).** Regardless of any attempt to conceal or disguise the criminal origin of property, it is an offence to acquire, use or possess criminal property. This offence does not require the laundering process to be actively undertaken;
- **Tipping Off (subject to a maximum 5-year jail term and/or a fine).** It is an offence for anyone to take any action likely to prejudice an investigation by informing the person who is the subject of a suspicious activity report, or anybody else, that a disclosure has been made, or that the police or customs authorities are carrying out or intending to carry out a money laundering investigation;
- **Failure to Report (subject to a maximum 5-year jail term and/or a fine).** It is an offence to turn a 'blind eye' to money laundering. It is a criminal offence for persons working in the regulated sector to fail to report where they have knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering;
- **Laundering Terrorist Property (subject to a maximum 14-year jail term and/or a fine).** It is an offence to enter into or become concerned in an arrangement which facilitates the retention or control of terrorist property by concealing, removing it from the jurisdiction, transferring it to nominees or in any other way.

7. Risk-Based Approach

The Company applies a risk-based approach with regards to its AML/CTF strategy and routinely identifies and assesses the money laundering and terrorist financing risk the business is exposed to.

In assessing and identifying such risks, the Company takes into consideration the following factors:

- Risks posed by the Company's clients and any underlying beneficial owners;
- Countries or geographic areas on which the Company's clients operate and their proximity – geographically, culturally and historically – to higher-risk jurisdictions;
- Products and services offered by the Company;
- Transactions the Company executes on behalf of the clients;
- Delivery channels the Company uses.

The Company has identified the most potent money laundering and terrorist financing risks and implemented a range of mitigation measures. The complete list of risks is provided in the Procedures.

The other risks the Company's business may be exposed to are:

- Reputational risk;
- Bribery risk;
- Fraud risk;
- Corruption risk.

7. Due Diligence

The Company is required to undertake appropriate due diligence measures across its client base to ensure the Company has undertaken a comprehensive appraisal of all potential clients. To do this, the Company will establish and verify their identity, assets, nature and intended purpose of the relationship and liabilities. The Company adopts a risk-based approach to determine the level of due diligence required for each type of clients and the potential money laundering and terrorist financing risk they pose to the business.

The information about the client due diligence checks shall be recorded in the customer relationship management system employed by the Company.

In evaluating the risk level of each client, the Company will consider risk factors surrounding the client, the product/service they are acquiring, the anticipated frequency and volume of transactions and their geographical location.

7.1 Three Levels of Due Diligence

The Company will conduct one of three levels of due diligence depending on the outcome of each client's risk assessment:

Simplified Due Diligence

Simplified due diligence is the lowest level of due diligence that can be completed on a client. Before conducting simplified due diligence on a client, a risk assessment is required to demonstrate that the client presents a lower degree of risk and requires suitable ongoing monitoring. As such, simplified due diligence is reserved for clients who present a low risk of money laundering or terrorist financing and where this low risk can be evidenced.

Following the 4MLD's implementation in June 2017, simplified due diligence is no longer automatically available to clients such as FCA-regulated firms, UK public authorities and UK pension schemes. Such clients must now pass through the risk assessment process.

Standard Due Diligence

The standard due diligence involves the essential measures, taken by the Company in accordance with the Applicable Regulation, to establish the identity of the clients and, where applicable, their principals and respective beneficial owners. All identification data has to be verified. The identity will be established and verified to the Company's satisfaction by reference to the reliable, independent source documents, data or information. The detailed list of information and documents required to establish and verify the identity of various groups of clients is available in the Procedures.

As no single form of identification can be fully guaranteed as genuine, or representing correct identity, the identification process will need to be cumulative, and no single document or source of data (except for a database constructed from a number of other reliable data sources) must therefore be used to verify both name and permanent address.

Should there be any doubt about the validation of the client's identity the Enhanced Due Diligence measures should be undertaken.

Since the passing of 4MLD, standard due diligence must be obtained in relation to regulated firms taken on as clients. This is likely to take the form of a check against the FCA Financial Services Register

(or another regulatory record, as required), combined with the obtaining of client legal documents such as memoranda and articles and documentary evidence of the identity of the individuals representing the client firm.

Enhanced Due Diligence

The enhanced due diligence will be required when the risk assessment has ascertained that the client poses a high risk of money laundering or terrorist financing to mitigate the increased risk to the business. The Company may apply the enhanced due diligence measures where:

- The client is or may be a PEP;
- The client is based in a high-risk country or is involved in transactions between parties based in high-risk third countries;
- The client performs large or complex transactions that cannot be explained when considering the client's transaction history;
- The client is the beneficiary of a life insurance policy;
- The client is a third-country national seeking residence rights or citizenship in exchange for transfers of capital, purchase of a property, governments bonds or investment in corporate entities;
- There are non-face to face business relationships or transactions without certain safeguards, for example, as set out in Regulation 28 (19) of MLR concerning electronic identification processes;
- The client is involved in transactions related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory or other items related to protected species, or archaeological, historical, cultural and religious significance, or of rare scientific value.

The enhanced due diligence implies taking additional steps in relation to client identification and verification of identity and may include the measures specified in the Procedures.

All clients who require the enhanced due diligence must be signed off by the MLRO before any transactions take place.

7.2 Politically Exposed Persons (PEPs)

When a valid PEP or family member or close associate of a PEP, has been identified the MLRO is required to approve the initiation of the bespoke business relationship. This includes the continuation of a relationship with an existing client who may be identified as a PEP following the initial client on-boarding process. In the event that the Company identifies a PEP, it will conduct enhanced due diligence determined on a risk-sensitive basis.

The Company will initially be made aware of a potential PEP status following the application of the appropriate due diligence measures across the Company's entire client base and during the initial onboarding process. The Company will then conduct a full media search on the potential PEP before assessing whether it is a 'true match'. The results of this search are to be submitted to the MLRO for consideration.

7.3 Beneficial Ownership

According to the Applicable Regulation, the 'beneficial owner' generally means an individual who ultimately owns or controls the entity or arrangement or on whose behalf a transaction is being conducted. The Company has an obligation to identify and verify the identity of any beneficial owner of any entity on whose behalf a transaction is being conducted.

According to the Applicable Regulation, the Company shall obtain and hold adequate, accurate and current information on beneficial ownership and control structure of corporate clients, including the

details of the beneficial interests held. The Company shall record any difficulties encountered in identifying beneficial ownership of the corporate clients.

The information about the corporate clients shall be checked against the information available in the central register, which is maintained and controlled by the Companies House, and any discrepancies shall be reported to the Companies House.

The central register is located at: https://companieshouse.blog.gov.uk/2016/04/13/the-new-people-with-significant-control-register/.

8. Suspicious Activity Reports (SARs)

The Company requires that anyone who knows or suspects, or has reasonable grounds for knowing or suspecting, that a client is engaged in money laundering or terrorist financing, has an obligation to report this information to the MLRO as soon as is reasonable practical after the information comes to them. Internal SARs to the MLRO must be made regardless of whether the transaction has taken place.

The MLRO must consider each internal SAR and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for the knowledge or suspicion of money laundering or terrorist financing. When considering an internal SAR, the MLRO should make every endeavour to collect as much information as possible regarding the client/transaction but in the interest of timely reporting, may need to consider making an initial report to the NCA prior to the full review of linked/connected relationships and transactions.

The Company fully understands that it is an offence to 'tip-off' (i.e. inform) a person suspected of money laundering or terrorist financing that an investigation in their business relationship or transactions is taking place. Under no circumstance may the individual under suspicion, be informed of a pending investigation. All relevant staff have been made aware of the penalties for tipping-off and potentially jeopardising an investigation of the client's suspicious activity.

Where the MLRO concludes that the internal SAR does give rise to knowledge or suspicion of money laundering or terrorist financing, he must make a report to the NCA as soon as is practicable after he makes this determination. In some instances, the MLRO may allow the transaction to proceed subject to obtaining consent from the NCA.

9. Client Screening

The Company is required to comply with the UK's financial sanctions regime and recognises its responsibility to deny services and products to individuals who pose a significant money laundering and terrorist financing risk to the UK and the international financial system.

To comply with the regime, the Company applies credible procedures to screens the clients being on-boarded by the Company and then at regular intervals, either upon a trigger event or as the client's / Sanction Lists' information changes, to validate that the relationship remains permissible.

The screening involves checking of client's name against:

a) Most up-to-date consolidated list of sanctions targets issued by the OFSI and international sanctioning bodies. Such consolidated lists are available to the Company through the Screening Software.

b) Lists of Terrorists, which are available on the following websites:

   http://www.statewatch.org/terrorlists/thelists.html
   https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx
   https://www.fbi.gov/wanted/wanted_terrorists.

As part of the screening process, close attention is paid to the jurisdictions, such as NCCTs, which have been earmarked by international organisations as having AML/CTF regimes considered to be strategically deficient. FATF frequently publishes documentation available on its websites, which identifies and evaluates such jurisdictions

The client screening is undertaken manually by a dedicated Company officer. The Company ensures that such an officer has the appropriate skills and experience in understanding the nuances of sanctions requirements and how these might influence screening outcomes and decisions, as well as technical capabilities of Screening Software.

Where an alert has been generated by the LexisNexis Platform as a result of the client's name screening, the dedicated Company officer shall collect additional information on the particular client to evaluate whether the similarities in the text reveal a true sanctions match.

Where the dedicated Company officer has identified a true client's name match on either list included in the Screening Software, he shall immediately make the MLRO aware of this finding.

The Company shall inform the HMT's Asset Freezing Unit as soon as practicable where is has identified an actual match with a person or entity on the HMT list.

The Company carries out regular (every 6 months) review of the appropriateness of the screening and monitoring systems to ensure that they remain up-to-date and effective.

10. Transaction Monitoring

The Company is required to conduct ongoing monitoring of the business relationship with all of its clients. This ongoing monitoring entails:

- Scrutiny of transactions undertaken throughout the course of the relationship (including a source of funds) to ensure the transactions are consistent with the Company's knowledge of the client;
- Ongoing monitoring of payment instructions to ensure that proposed payments to any Sanctioned persons or their agents are not made;
- Ensuring that the client documentation obtained for the purpose of applying the necessary due diligence measures remains up to date;
- Reassessing the risk associated with the business relationship where monitoring indicates material changes to a client's profile.

The transaction monitoring is performed manually by the dedicated Company officer in accordance with the Procedures.

Any transactions or activities which are not consistent with the client's business and risk profile are flagged for further examination by compliance and the client's account will be frozen. Where the decision is made by the Company to freeze a client's funds under the financial sanctions regime, the Company must make a report to OFSI and/or NCA.

Any actions undertaken by the dedicated Company officer, the MLRO, the Board or any other representative of the Company with regard to the transaction (collecting additional information, submitting internal or external SAR etc.) shall be thoroughly documented in order to keep a transaction audit trail for review as part of effectiveness and quality assurance process as well as evidence for audit and regulatory purposes.

11. Training

All staff and contractors of the Company should be made aware of the Applicable Regulation, about how to identify suspicious activity and the obligations placed on the Company. They should also be aware of the identity of the MLRO.

All staff requires training covering the Company's procedures and how to recognise and deal with suspected Money Laundering or Terrorist Financing concerns.

Staff training records are to be retained and evidenced on each individual employee's Continual Professional Development (CPD) Log alongside the Company's central training log. Records are required to be retained for five years.

12. Record-Keeping

In line with the Applicable Regulations, the Company will retain the required client records for five years following the termination of a business relationship or occasional transfer, except for situations where legal obligations placed upon the Company require otherwise. The required client records, as specified in regulation 40(2) of the MLR, include:

- A copy of any documents or information obtained by the Company to satisfy the client due diligence requirements (including recorded information provided over the phone).
- Sufficient supporting record in respect to transactions which are subject to the client due diligence measures.