Pepperstone

ANTI-MONEY LAUNDERING & COUNTER TERRORISM FINANCING POLICY

Company:	Pepperstone EU Limited
Reg. Number:	HE 398429
CySEC Licence:	388/20
Version:	1.0
Review:	Annual
Date Updated:	1 October 2020

Table of Contents

1. Introduction

This policy outlines Pepperstone EU Limited ("Pepperstone" or the "Company") approach to preventing and detecting Money Laundering and Terrorist Financing. In developing this policy, Pepperstone considered all current Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) obligations required in the Cyprus Law 188(I)/2017 as amended (the "Law"), the 4th EU AML Directive as well as best regulatory guidance issued the Cyprus Securities and Exchange Commission "CySEC" in the form of Directives and Circulars.

Pepperstone 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, Pepperstone is committed to fostering and promoting a compliance culture throughout the firm which underpins the importance of preventing Money Laundering and Terrorist Financing.

Pepperstone recognises it has a statutory duty under Cyprus Law to prevent the facilitation of its services for Money Laundering and Terrorist Financing purposes. Subsequently, Pepperstone pledges to allocate sufficient resources into the firm's internal controls, monitoring system, human resources and staff training to prevent financial crime.

1.1 Scope

All employees, directors, officers and associated agents are required to comply with these policies. Failure to do so may result in disciplinary action.

1.2 Objective

The objectives of the policy are to:

- Emphasise our stringent commitment to preventing Pepperstone 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 Pepperstone has implemented to prevent and detect Money Laundering and Terrorist Financing.
- Clearly outline the responsibilities of the firm's senior management, Money Laundering Reporting Officer ("MLRO") and other key individuals in relation to the firm's AML/CTF strategy.
- Explain the most up-to-date Money Laundering and Terrorist Financing risks that Pepperstone is vulnerable to and how the firm intends to counteract these risks.

- Confirm that Pepperstone will take steps to monitor compliance with this policy throughout the firm.

2. What is Money Laundering?

Pepperstone views Money Laundering to be: 'the process by which illegally gained proceeds or funds are cleansed 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.

2.1 Three Stages of Money Laundering

The Money Laundering process traditionally follows three stages:

Placement

The placement stage represents the initial entry of proceeds derived from 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?

Pepperstone 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.

Pepperstone 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 AMLCO & Senior Management

Pepperstone clearly defines the roles and responsibilities of all individuals with oversight of the firm’s AML/CTF strategy and responsibility for the firm’s compliance with all AML/CTF requirements.

4.1 AMLCO

Pepperstone Board of Directors appoints a senior management individual as the Company’s Anti Money Laundering Compliance Officer (AMLCO). The AMLCO will assume responsibility for the firm’s AML/CTF strategy.

It is the AMLCO’s responsibility to oversee the Company’s compliance with the Money Laundering regulations. The AMLCO is responsible for:

- Receiving and investigating internal reports relating to (suspicions of) Money Laundering and Terrorist Financing.
- Making reports of relevant suspicious activity to the Unit for Combating Money Laundering (MOKAS);

- Ensuring 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 firm.
- Reporting at least annually to the board on the operation and effectiveness of the firm's AML systems and controls.
- Responding promptly to any reasonable requests for information made by a regulator of the firm.
- The approval and risk assessment of new or amended products/jurisdictions/sales channels.
- Approving business relationships which the firm wishes to enter or continue where the consumer is a Politically Exposed Person ("PEP").
- Approving business relationships which the firm wishes to enter or continue where the consumer resides in or trades with a jurisdiction which is considered by Financial Action Task Force (FATF) as non-cooperative or has a high risk of terrorism.
- Establishing and maintaining policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in any risk assessment.
- Communicating the policies, controls and procedures which the firm establishes and maintains in accordance with this regulation to relevant personnel of the Company.

Appointment of Alternate AML Compliance Officer

- In accordance with CySEC AML Directive, Pepperstone should appoint an Alternate AML Compliance Officer, to temporarily replace the AMLCO when the AML Compliance Officer is absent. It is clarified that the provisions of paragraph 8 of the Directive do not apply when the AML Compliance Officer resigns from his position, since in such case Pepperstone is required to appoint a new AML Compliance Officer, always subject to CySEC prior notification and approval as required by the applicable law and the CySEC AML Directive.
- Pepperstone is required to inform CySEC and submit the name, position and contact details of the Alternate AML Compliance Officer.

4.2 Senior Management

Pepperstone appoints a Board member to assume responsibility for the firm's compliance with the Anti-Money Laundering regulatory framework (the "AML Director").

Overall, Pepperstone's AML Director together with senior management is responsible for:

- Ensuring that the firm's AML/CTF policies, procedures and controls are appropriately designed and implemented to reduce the firm's vulnerability to Money Laundering and Terrorist Financing.
- Being fully engaged in the decision-making process regarding the firm's AML/CTF strategy and take ownership of their risk-based approach.
- Being involved in the design of the firm's policies, procedures and controls and approving them.
- Being aware of the level of Money Laundering and Terrorist Financing risk the firm is subject to.
- Ensuring that the firm fulfils their obligations under the Cyprus AML Law, the 4th AML Directive and CySEC related Directive and Circulars.

4.3 Employees Training

All Pepperstone's employees are trained to identify and report suspicious activity. They are also given regular training on the law relating to Money Laundering and Terrorist Financing.

5. Regulatory Responsibility

Pepperstone EU Limited is registered with the CySEC, licence number 388/20.

6. Regulatory Framework

Pepperstone is fully aware of the Cyprus and EU regulatory framework relating to AML and CTF. Pepperstone also provides regular training to our employees, agents and subsidiaries to ensure they have sufficient knowledge of the applicable regulatory framework.

Pepperstone is required to adhere to the following legislation and regulations:

- Directive (EU) 2015/849 (4th AML Directive) of the European Parliament and of the Council and Directive (EU) 2018/843 amending Directive (EU) 2015/849
- The Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007-2019 (Law 188(I)/2007 and subsequent amendments)
- CySEC Directive for the Prevention and Suppression of Money Laundering and Terrorist Financing "the Directive"
- Any Circulars and guidelines issued by CySEC in relation to Anti-Money Laundering such as Circulars CI1442014-25, C033, C292, C296, C299, C300, C303, C307, C314, C317, C318, C319, C337, C339 and C367.

- Guidance of other relevant global bodies such as The Joint Money Laundering Steering Group (JMLSG) Guidance is also considered as a consulting tool.

6.1 Offences

The above legislation and regulations outline multiple Money Laundering and Terrorist Financing offences, which Pepperstone is committed to avoiding. The key offences under the applicable legislation and regulation, which are subject of up to a maximum of 14-year imprisonment and/or a fine of up to EUR 500.000 are as follows:

- **Concealing**
    - It is an offence to help conceal, disguise, convert, transfer or remove funds from the Republic of Cyprus if you know, should have known, suspect or should have suspected that the funds were the proceeds of criminal conduct.
- **Arrangements**
    - 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**
    - 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**
    - 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. MOKAS or any other relevant authorities are carrying out or intending to carry out a Money Laundering investigation.
- **Failure to Report**
    - It is an offence to ‘blind eye’ to money laundering by making it 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**
    - 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

Pepperstone 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.

As required under the Anti-Money Laundering regulatory framework, Pepperstone will conduct a regular risk assessment to examine all risks of Money Laundering and Terrorist Financing to which to business is subject. In assessing and identifying such risks, the firm will take into consideration the following factors:

- Risks posed by the firm's clients.
- Products and services offered by the firm.
- The geographical areas of the firm's clients.
- Delivery channels the firm uses.
- The volume and complexity of the client's transactions.

Once the risks have been identified and assessed, Pepperstone pledges to amend its policies, procedures and controls in accordance with the underlying risks.

7.1 Risks Identified

Pepperstone has conducted a risk assessment to identity the most potent Money Laundering and Terrorist Financing risks for the which the firm is vulnerable. A full list of risks identified by the firm in its most recent risk assessment can be found in the AML and CTF Risk Assessment.

7.2 How will the Company Mitigate Risks?

Pepperstone has implemented numerous measures to counteract the risk of Money Laundering and Terrorist Financing through the firm. A full list of risks identified by the firm in its most recent risk assessment can be found in the AML and CTF Risk Assessment.

7.3 Main components of the AMF and CTF framework for high risk clients

Concerning the Money Laundering and Terrorist Financing threat that certain designated high-risk clients pose, Pepperstone will apply a four-component framework to enhance its Anti-Money Laundering actions.

The four main components that Pepperstone will apply are as follows:

Customer Due Diligence

Undertake enhanced customer due diligence measures before entering into a transaction or business relationship or during a business relationship with a designated high-risk person.

Ongoing Monitoring

Undertake enhanced ongoing monitoring of any business relationship with a designated high-risk person.

Systematic Reporting

Collect enhanced information and documents and perform enhanced reporting to senior management in relation to transactions and business relationship with a high-risk person.

Limiting or Ceasing Business

Do not enter or discontinue a transaction or business relationship with a high-risk person when directed by the AMLCO or Senior Management.

8. Due Diligence

Pepperstone is required to undertake appropriate due diligence measures across its customer base to ensure the firm has undertaken a comprehensive appraisal of all potential customers. To do this, the firm will establish and verify their identity, assets, the nature and intended purpose of the relationship and liabilities. Pepperstone adopt a risk-based approach to determine the level of due diligence required for each type of customer and the potential Money Laundering and Terrorist Financing risk they pose to the business.

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

8.1 Simplified and Enhanced Levels of Customer Due Diligence

Pepperstone will conduct distinct levels of due diligence depending on the outcome of each customer's risk assessment (i.e. low, medium, or high risk):

Simplified Due Diligence (SDD)

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

When applying "SDD" we need to verify customer's identity and comprise the risk profile of the customer. To complete "SDD", the customer's ID must be sought. This could include Pepperstone requesting a physical copy of the customer's government issued ID and/or by performing electronic Know Your Customer ("KYC") checks. Further we need to obtain at least a Proof of Address (POA) document.

When the client is categorised as Medium risk the ID verification is enhanced by requesting an additional ID document from the client for cross reference and requesting information about the customer's source of wealth/funds.

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

Enhanced Due Diligence

Enhanced Due Diligence ("EDD") will be required when the risk assessment has ascertained that the customer poses a high risk of Money Laundering to mitigate the increased risk to the business. This includes, but is not limited to, customers that are or may be Politically Exposed Persons and/or Sanctioned individuals.

In addition, customers found to be residing in/transferring to high risk countries and customers performing large or complex transactions that cannot be explained when considering the client's transaction history will also be subject to EDD by Pepperstone.

What EDD entails will be dependent on the nature and severity of the identified heightened risk. This could include, but is not limited to, obtaining additional ID evidence, ID verification, and a full description of source of wealth and funds, internet searches for potential negative screening, verifying additional information from the customer about the purpose and

intended nature of the transaction or the business relationship and after establishing the relationship, increasing the frequency and intensity of transaction monitoring.

All EDD customers must be approved by Pepperstone's AMLCO before the relationship is finalised and before any transactions take place.

Individuals or legal entities sanctioned by the EU or the UN are not accepted as clients.

8.2 Politically Exposed Persons ("PEPs")

When a valid PEP, or family member or close associate of a PEP, has been identified, Pepperstone's AMLCO 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. If Pepperstone identifies a PEP, the firm will conduct EDD measures determined on a risk-sensitive basis.

Pepperstone agrees with the definition of PEP given by the Financial Action Task Force (FATF), and the 4th EU AML Directive which is: 'an individual who is or has been entrusted with a prominent public function'.

Pepperstone will initially be made aware of a potential PEP status as a result of the AML checks which is completed across the firm's entire customer base and during the initial on-boarding process. Pepperstone 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 AMLCO for consideration.

8.3 Beneficial Ownership

A "beneficial owner", is defined as the individual who ultimately owns or controls the entity (in general with a percentage of 25% or more) or arrangement on whose behalf a transaction is being conducted. The regulatory framework places an obligation on financial institutions to identify and verify the identity of any beneficial owner of any entity on whose behalf a transaction is being conducted.

9. Suspicious Activity Reports

Pepperstone's AMLCO must report to the Unit for Combating Money Laundering (MOKAS) any transaction or activity that, after their evaluation, they know or suspect, or have reasonable grounds to know or suspect, may be linked to Money Laundering and Terrorist Financing. This is done by means of a Suspicious Transaction Report ("STR"). Such reports

should be made as soon as is reasonably practicable upon receiving the notification of suspicion. Pepperstone's AMLCO must consider each report of suspicious activity from within the firm and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for the knowledge or suspicion of Money Laundering or Terrorist Financing. Any approach to the customer or to the intermediary should be made sensitively by someone other than the AMLCO, to minimise the risk of alerting the customer or an intermediary that a disclosure to the MOKAS is being considered. Under no circumstance, is the individual under suspicion to be informed of a pending investigation.

Pepperstone fully understands that it is an offence to "tip-off" (i.e. inform) a person suspected of Money Laundering that an AML investigation in their business relationship or transactions is taking place. All relevant staff have been made aware of the penalties for tipping-off and potentially jeopardising an AML investigation. For further clarity regarding tipping-off, please contact the firm's AMLCO.

When considering an "Internal Suspicion Report", the AMLCO should make every endeavour to collect as much information as possible regarding the customer/transaction but in the interest of timely reporting, may need to consider making an initial report prior to the full review of linked/connected relationships and transactions.

Internal Suspicion Reports to the AMLCO must be made regardless of whether the transaction has taken place. In some instances, it may be necessary for the AMLCO to obtain consent from the MOKAS prior to continuing with the transaction.

A templated "Internal Suspicion Report" has been included as Appendix A.

10. Sanctions Screening

Pepperstone is required to comply with the European Union (EU) and the United Nations (UN) 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 international financial system.

To comply with the regime, Pepperstone screens all persons being on-boarded by the firm against the most up-to-date consolidated list of sanctions targets issued by the EU or the UN. Pepperstone then also screens all clients on a weekly basis to ensure someone has not be added to the sanction list after they have been onboarded as a client. Pepperstone also allocates adequate resources on areas of the business that carry a greater likelihood of involvement with targets or their agents. As part of the firm's controls, Pepperstone monitors payment instructions to ensure that proposed payments to targets or their agents are not made.

Pepperstone pays close attention to jurisdictions which have been earmarked by international organisations, such as FATF, as having AML/CTF regimes considered to be strategically deficient. FATF frequently publishes documentation available on its websites which identifies and evaluates such jurisdictions.

FATF uses these publications to signal to its members and other jurisdictions to apply countermeasures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing risks emanating from these countries.

FATF publishes a list of jurisdictions which have strategic AML/CFT deficiencies for which they have developed an action plan with FATF. This list can be found at: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

10.1 Terrorist Lists

The acts of terrorism committed against the USA in September 2001 have increased the international efforts to locate and cut off funding for terrorists and their organisations. Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move those funds between jurisdictions. In doing so, they require the services of skilled professionals such as bankers, accountants and lawyers.

The sites below confirm lists of international terrorists:

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

Pepperstone understands it is an offence to provide financial services to any suspected or known terrorists and implements measures to prevent this eventuality.

11. Monitoring, Management Information & Reporting

Pepperstone's AMLCO must ensure that all systems, controls, policies and procedures are up-to-date and compliant to the regulatory framework.

At least once in each calendar year, the firm's AMLCO will provide a report to the governing body and senior management. The report must include the following:

- Review of the effectiveness of the firms AML systems and controls, with appropriate recommendations for improvement in the management of risks and priorities, including resources.
- Detail those within the firm responsible for AML systems and controls.
- Concluding actions and the remedial progress in response to these is to be stored in a secure location central to the business.
- It must indicate the way in which new findings on countries with AML inadequacies have been used during the year.
- The number of internal reports made by staff.

Pepperstone's senior management will give these reports due consideration and take necessary actions to remedy any deficiencies identified by the report.

The firm has an obligation to regularly update the CySEC on the systems and controls we have in place to prevent financial crime and how the firm mitigates the risk of financial crime. As such, Pepperstone's AMCLO is required to submit the annual AMLCO report to the CySEC.

The policies, procedures and controls that Pepperstone have in place are regularly amended and enhanced in accordance with updates to legislation, regulation, and industry best practice. Our systems and controls also change to counteract the risks identified by the firm in its regular risk assessments. Subsequently, Pepperstone has systems in place to monitor staff compliance with the firm's policies, procedures and controls.

12. Ongoing Monitoring of Customer Activity

Pepperstone is required to conduct ongoing monitoring of the business relationship with all of its customers. As per the regulatory guidance, this ongoing monitoring entails:

- Scrutiny of transactions undertaken throughout the course of the relationship (including source of funds) to ensure the transactions are consistent with the firm's knowledge of the customer.
- Ensuring that the documentation obtained for the purpose of applying Client Due Diligence remains up to date.

It is essential for the firm's monitoring system to have the following features:

- Flags up transactions for further examination.
- These transactions are reported to and reviewed promptly by the authorised person(s).
- Appropriate action is taken on the findings of any further review.

Pepperstone's monitoring system for customer activity is based on the following risk factors:

- The unusual nature of the transaction. E.g. an abnormally large transaction not consistent with the firm's knowledge of the customer.
- The number of a series of transactions. E.g. many small transactions initiated in quick succession.
- The geographical destination or origin of a payment. E.g. a payment to a high-risk jurisdiction.
- The parties concerned. E.g. a request to make payment to or from a person on a sanctions list.

A full list of Pepperstone's ongoing monitoring systems and methods can be observed in the AML and CTF Risk Assessment.

13. Training

All staff and contractors of Pepperstone should be made aware of the laws and regulations surrounding Money Laundering and Terrorist Financing, how to identify suspicious activity, and the obligations placed on the firm. They should also be aware of who has been appointed as the firm's AMLCO.

All staff require training covering the firm'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 firm's central training log. Records are required to be retained for five years.

14. Record-Keeping

In line with the EU regulatory framework, Pepperstone will retain customer information for five years following the termination of a business relationship or occasional transfer, except for situations where legal obligations placed upon Pepperstone require otherwise. Where the record keeping obligations under the ML Regulations are not observed, a firm or person is open to prosecution and/or a fine.

15. Review of Policy

In line with the EU regulatory framework, Pepperstone's AMLCO will review this policy at least annually and any change shall be approved by the Board of Directors.

Appendix A: Money Laundering Suspicious Activity Report Form

Note that should you advise the customer or anyone else of your suspicion and report, you may be committing the criminal offence of tipping off.

All reports are treated in confidence. None of your details are forwarded outside of Pepperstone

Please complete both sides and use BLOCK CAPITALS.

Completed Money Laundering Suspicious Activity Report Forms should be forwarded to:

Mr. Stavros Vassiliades, AMLCO,
Email: stavros.vassiliades@pepperstone.com
Post Address: Pepperstone EU Limited, 3rd Floor Metis Tower 363, 28th October Avenue, Limassol, 3017 CYPRUS

SUSPICIOUS ACTIVITY REPORTING FORM

REPORTED BY	
Name	
Position & Department	
Phone no.	

CLIENT DETAILS	
Name	
Account Number	
Address	

Date of birth	
Nationality	
Email address	
Contact number	
Occupation & Employer	
Existing or new client	
User ID	
How was the client identified? (Reasons for Suspicion)	

ASSOCIATED PERSON(S) DETAILS (IF APPLICABLE)	
Name	
Account Number	
Address	
Date of birth	
Nationality	
Email address	

Contact number	
Occupation & Employer	
Existing or new client	
User ID	
How was the client identified? (Reasons for Suspicion)	

TRANSACTION DETAILS					
No	**Date**	**Amount**	**Payment method**	**Card ending**	**Status**
1					
2					
3					
4					
5					
6					
7					
8					

9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					

25					

REASON FOR SUSPICION

SIGNATURE	
Signature	
Date	

DO NOT ADVISE THE CLIENT OR ANYONE ELSE WHO DOES NOT NEED TO KNOW OF YOUR SUSPICION AND REPORT

3rd Floor Metis Tower
363, 28th October Avenue
Limassol, 3107
CYPRUS

Phone +357 25 030573

www.pepperstone.com
support@pepperstone.com