# FINANCIAL CRIME POLICY AND PROCEDURES

Version: 1.3

December 2022

# Contents

Background Documents Reference

1. The Money Laundering Regulations 2007 (‘MLR’)
2. EC Regulation 1781/2006 on information on the payer accompanying transfers of funds (commonly known as the Payments Regulation or the Wire Transfer Regulation)
3. Transfer of Funds (Information on the Payer) Regulations 2007
4. SRC: MLR8 Preventing money laundering and terrorist financing [August 2008]
5. Guidance issued by the Joint Money Laundering Steering Group (‘JMLSG’) on ‘Prevention of money laundering/combating terrorist/financing’ [November 2009].
6. Proceeds of Crime Act 2002 (as amended) (‘POCA’)
7. Terrorism Act 2000, and the Anti-terrorism, Crime and Security Act 2001
8. Counter-Terrorism Act 2008, Schedule 7
9. Financial sanctions
10. The Bribery Act 2010
11. The Fraud Act 2006

# 1 Introduction

## 1.1 Guidance

The primary purpose of this Financial Crime Guidance (the ‘Guidance’) is to document the approved Policy and guidance of ForexVox (Seychelles) Financial Services Ltd. (“Company”), **relating to:**

- Financial crime – Preventing Company’s association with money laundering,terrorist financing, fraud, and bribery & corruption
- Establishing new customer relationships
- Monitoring of existing customer relationships

**In addition, the Guidance:**

- Identifies and provides guidance on implementing the key internal procedure and controls in support of the anti-money laundering (‘AML’) framework
- Confirms the determination of Company’s senior management to prevent andimplement measures to counter financial crime

## 1.2 Financial crime policy statement

The Directors and Senior Management Team ('SMT') are responsible for assessing money-laundering risk and ensuring appropriate implementation of risk-sensitive policy and procedure within the business. The Board fully supports the UK's AML regime and has zero tolerance for criminal use, or misuse, of Company's services infurtherance of money laundering.

**The Board is committed to ensuring that:**

- The risk of the Company being used as a vehicle for money laundering or terroristfinancing is minimized
- Appropriate knowledge and awareness is maintained in the business, of the UK's anti-money laundering ('AML') requirements and relevant law
- Where transactions suspected to involve money laundering are recognised, these will be reported to the appropriate authorities, including any linked to persons or entities suspected of being involved in or supporting acts of terrorism
- Should a customer of the firm come under investigation by law enforcement, the Company will be able to provide its part of any relevant audit trail, in respectof transactions or information about the customer, held by the firm

**The Board expects all Directors, managers and employees to:**

- Comply with Company's Financial Crime Policy Statement ('the Policy')
- Attend and complete relevant training provided by the firm, including AML training
- Be alert to money laundering, fraud and other forms of financial crime, including bribery & corruption, and financial sanctions risk; and to report incidents or suspicions to management (as per this Guidance)
- Ensure timely reporting to the Nominated Officer of all money laundering suspicions identified in any transaction/arrangement associated with Company's business.

## 1.3 The Company

### 1.3.1 Company name & Principal Place of Business:

ForexVox (Seychelles) Financial Services Ltd.

CT House, Office 8G, Providence, Mahe, Seychelles

### 1.3.2 Authorisation and licensing:

The Company is authorised to

- Arranging (bringing about) deals in investments
- Making arrangements with a view to transactions in investments
- Dealing in Investments as Agent
- Arranging safeguarding and administration of assets
- Dealing in investments as Principal (matched principal limitation)
- Agreeing to carry on a regulated activity

The core service which is offered by the Company is providing execution-only retail derivative products.

**As a regulated firm, the Company is required, to:**

- Appoint a Nominated Officer/ Money Laundering Reporting Officer
- Assess money laundering risk associated with the firm's customers
- Implement risk-sensitive procedures, which serve to reduce the risk of the business being used by money launderers and terrorists, including procedures linked to:
  - Customer take-on
  - Account monitoring arrangements
  - Record retention
- Provide relevant training to management and employees

# 2 Money laundering

## 2.1 What is money laundering?

Money laundering includes all forms of handling or possessing criminal property, including possessing the proceeds of one's own crime, and facilitating any handling or transfer of criminal property for another person; including the proceeds derived from any act of fraud, bribery or corruption. Where criminal property includes money or money's worth, securities, tangible and intangible property; including the receipt, handling and transfer of funds derived from criminality.

A simplified view of an effective money laundering operation involves three stages:

- Placement of physical cash (e.g. in a bank account)
- Layering - By using funds from the bank account and undertaking multiple transactions which confuse the audit trail and separate the money from its origin
- Integration of laundered proceeds into the legitimate economy, so that it appears to be legitimate by being presented as normal business funds

For the purpose of this Guidance, money laundering also includes activities relating to terrorist financing, including handling or possessing funds to be used for terrorist purposes as well as proceeds from terrorism.

When dealing with customers (or new applicants for business) you need to be alert to the possibility that customers, their counterparties or others (with or without the customer's knowing participation) may try to launder money using the firm's services - by way of layering or integration.

## 2.2 Money Laundering Offences

The Proceeds of Crime Act ('POCA') includes various criminal offences related to money laundering, including:

A person may commit a money laundering offence[1] if he:

- Conceals, disguises, converts or transfers criminal property, or removes criminal property
- Enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person (s328)
- Acquires, uses or has possession of criminal property except where adequate consideration was given for the property (s329)

In the case of terrorist financing The Terrorism Act 2000 ('TA 2000') includes offences related to involvement in providing money or other property for terrorist financing. The definition of 'terrorist property' means that all dealings with funds or property (which are likely to be used for the purposes of terrorism), even if the funds are "clean" in origin, is a terrorist financing offence.

Upon conviction on indictment penalties for some offences are punishable by up to 14 years imprisonment and/or an unlimited fine.

[1] Sections 327-329 in the Proceeds of Crime Act (POCA) (as amended by the Serious Organised Crime and Police Act 2005 (SOCPA))

**But, under POCA, an offence may not be committed where:**

- Persons did not know or suspect that they were dealing with criminal property
- A report of a suspicion identified is made promptly to the firm's MLRO (an internal report) or direct to NCA (a suspicious activity report, or SAR), and (if the report is made before the act is committed) the appropriate consent is obtained before doing the act
- No report is made, with a reasonable excuse for the failure (e.g. under duress, threat or intimidation - might be acceptable reasons)
- Conduct giving rise to the criminal property was reasonably believed to have taken place outside of the UK, and the conduct was in fact lawful under the criminal law of the place where it occurred, and the maximum sentence if the conduct had occurred in the UK would have been less than 12 months

With regards to terrorism and involvement in terrorist financing, ss15-18, Terrorism Act 2000 also creates similar offences to those contained in s327-329 (POCA).

## 2.3 Failing to disclose

Persons employed in the regulated sector commit an offence if they fail to make a disclosure in cases where they have knowledge or suspicion, that money laundering is occurring.

Similar provisions regarding failure to disclose are contained in s19, and 21A, Terrorism Act 2000. The s19 failure to report offence is applicable to anyone in employment or business outside of the regulated sector, with s21A being applicable to all those in the regulated sector.

A failure to disclose offence is committed if an individual fails to make a report comprising the required disclosure as soon as is practicable either in the form of an internal report to his MLRO or in the form of a SAR to a person authorised by NCA to receive disclosures.

**The obligation to make the required disclosure arises when:**

- A person knows or suspects, or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering
- The information or other matter on which a suspicion is based came to him in the course of business in the regulated sector
- He either can identify that other person, or has information concerning the

whereabouts of the laundered property or the information he has may assist in identifying the person or the whereabouts of the property (the laundered property is that which forms the subject matter of the known or suspected money laundering)

**When submitting an internal report to the MLRO:**

- MLROs have a duty to make disclosures under POCA or the Terrorism Act 2000, if they have knowledge, suspicion or reasonable grounds to suspect money laundering or terrorist financing, as a consequence of an internal report
- An MLRO may commit an offence if he fails to pass on reportable information in internal reports that he has received, as soon as is practicable, to NCA

## 2.4 Tipping-off

**A criminal offence of Tipping-off arises where a person in the regulated sector discloses either:**

- That a disclosure has been made by a person of information obtained in the course of a regulated sector business either to an MLRO or to NCA or to any other person authorised by NCA to receive disclosures, or to the police or SRC and the disclosure is likely to prejudice any investigation that might be conducted following the disclosure referred to
- That an investigation into allegations that a money laundering offence has been committed, is being contemplated or is being carried out and the disclosure is likely to prejudice that investigation and the information disclosed came to the person in the course of a business in the regulated sector

A tipping-off offence may not be committed if the person did not know or suspect that the disclosure was likely to prejudice any investigation that followed. However, the penalty for this offence under POCA, on conviction on indictment, is imprisonment for a term not exceeding two years, or a fine or both. The Terrorism Act 2000 has a similar tipping-off offence in relation to prejudicing terrorism investigations.

# 3 What are the money laundering risks

Execution only (ExO) brokers carry out transactions in securities with regulated market counterparties, as agent for individual customers. ExO transactions are carried out only on the instructions of the client.

Some ExO brokers deal with high volumes of low value customers transactions, whereas others direct their services towards higher net worth customers, and thus have fewer

customers. Customers may adopt a variety of trading patterns; the firm is offering no advice and may have little or no knowledge of a client's motives.

ExO Customers are also free to spread their activities across a variety of brokers for perfectly valid reasons and often do so. Each broker may therefore have little transaction history from which to identify unusual behaviour. Many firms provide ExO services on a non-face-to-face basis, including via the internet.

In view of the above, while broking may be considered lower risk than some financial products and services; the risk is not as low as providing investment management services to the same type of customers in similar jurisdictions.

# 4 Who is the customer for AML purposes

The typical customers for execution only retail broking are individuals. However, customers also include solicitors, accountants, IFA's, as well as trusts, companies, charities etc. Much execution only business can comprise of occasional, or linked, transactions of a value less than $15K (USD) which therefore may fall within the exemption in Part 1 of the JMLSG.

# 5 New customers

## 5.1 Client process

**At a high level the Company will undertake the following:**

- Customer Due Diligence is undertaken for all clients. The firm will obtain and verify evidence of primary and secondary ID to fulfil the Anti-Money laundering requirements. Additionally as the business model is based on non-Face to face relationships additional Enhanced Customer Due Diligence shall be performed on a risk based approach
- Check whether the client is a resident or a national of a noted "high risk" country then apply the required Enhanced Due Diligence before we accept them as our clients according to the risk based approach
- A Financial Sanctions check will be carried to check whether the client is on the financial sanctions register as published by the SRC or is a Politically Exposed Person

## 5.2 Verifying customer identity

Reasonable steps must be taken to check the client's identity to show that they are who they claim to be and if applicable that they are trading for a legitimate purpose.

All new clients must provide sufficient information for verifying their identity and formal identification of personal and address ID will be completed by the Company prior to any business being transacted. Guidelines for customer identification are providedbelow.

A risk-assessment will be undertaken to determine the extent of Continued Due Diligence ("CDD") required. In some cases this may provide for verification using a Simplified Due Diligence ('SDD') process, or for higher risk situations, via the application of Enhanced Due Diligence ('EDD').

The Compliance Department has overall responsibility for ensuring the completion of necessary identity verification before determining whether, from an assessment of the customer's risk profile and nature of services required, approval to commence a business relationship is deemed appropriate. This must be completed in all cases, without exception.

## 5.3 Simplified due diligence

Except where money laundering is suspected, SDD would normally apply

SDD might be applicable to customers, but should not automatically be assumed. Where an indicator or red-flag is present indicating a need for a higher degree of money laundering risk assessment, in such cases EDD must be applied (see below).

Whenever money laundering (or attempted money laundering) arrangement is suspected during the customer take-on process, the MLRO must immediately be notified.

## 5.4 Enhanced due diligence

The term 'enhanced due-diligence' ("EDD") officially means applying a rigorous and robust process of investigation over and above normal AML/KYC procedures, primarily taking reasonable steps to verify and validate a customer's identity.

It's the regulatory obligation of a financial institution to understand and monitor a customer's profile, business and account activity, specifically identifying irregular adverse information such as suspected fraud, money-laundering and/or terrorist financing. An "enhanced due-diligence" approach is designed to support actionable decisions to mitigate financial fraud, regulatory and reputational risk, as well as ensuring legal/regulatory compliance.

In addition to any situation which by its nature can present a higher risk of money laundering or terrorist financing, for three specific types of relationship EDD must be applied.

**These are:**

- Where a customer has not been physically present for identification purposes
- In respect of a correspondent banking relationship
- In respect of a business relationship or occasional transaction with a Politically Exposed Person ('PEP')

## 5.5 Non face-to-face business

The Company's operating model is built around non face-to-face contact with customers; predominantly via on-line contact. This means that the verification of information supplied by a customer on the account opening form, when confirming identity, must be based on reliable and independent sources.

**Online identity verification:**

- Is the preferred option for use with private individuals
- Provides speed of response and corroboration, independent of a customer, about identity and existence
- In some instances, partial on-line verification might be supported by hard copy documentation supplied by a customer

The Compliance function maintains details of the firm's approved provider(s) of electronic verification services, meeting the guidance and criteria of parts 5.3.35 to 5.3.40 of JMLSG Guidance

Where personal identity is verified electronically, the customer's full name, address and date of birth is to be used as the basis. Results of electronic verification must be consistent with a standard level of confirmation before being relied upon and also, used to assess the risk of impersonation fraud.

**The MLRO will ensure that persons reviewing results from the electronic verification service understand:**

- The system(s) used
- The format of search results
- Whether results can be relied on to confirm the standard identification requirement for private individuals

- Whether the results might indicate a risk of identity theft, or a need to apply EDD

Where an approved service provider verifies an individual's identity electronically, such as for that of a private individual or for one or more officers of a company, checks should use each person's full name, address and date of birth as a basis.

**To confirm identity, the standard level of confirmation required, is:**

- One match on an individual's full name and current address, **and**
- A second match on the full name and **either** his current address **or** his date of birth.

## 5.6 Additional measures

For all non-face-to-face verification of customer identity, Compliance will assess the need for any additional measure(s) to apply, in order to: mitigate the risk of impersonation fraud and money laundering; or to clarify any additional information that might be required when assessing applicant names against the SRC maintained list of financial sanctions.

Where necessary, Compliance will cause additional measures to be applied, in order to compensate for data anomalies or higher risk indicators - for example, by applying one or more of the following:

- Ensuring that the first sums received from a customer originate from an account opened in the customer's name with a recognised bank. Since 1 January 2007, EU regulation 1781/2006 requires credit institutions to provide the payer's name, address and account number with all electronic fund transfers. Verifying customer and payer details on the first payment received, should assist the Company to verify a client's identity
- Establishing telephone contact with the applicant (prior to opening the customer's account) via a home or business number which has been verified (electronically or otherwise), or holding a "welcome call" with the customer before transactions are permitted. Such contact can be used to verify additional aspects of personal identity information that have been previously provided during the setting up of an account
- Communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation, which, in full or in part, might be required to be returned completed or acknowledged without alteration)
- Conducting research into/about a company's business operations, including

research of news media and other open source material on the Internet, or via subscription based service providers. Information collated may be useful to identify the reputation and standing of the customer, those who represent the customer and/or those who do business with the customer

### 5.6.1 Verifying identity using customer documentation

Where on-line verification is not possible or impracticable, or fails this necessitates the receipt, review and handling of identity documents supplied by customers.

**By way of example, on-line verification may not be possible, due to:**

- Lack of availability of reliable data for use when confirming identity
- A customer having moved address recently with little, if any, electronic footprint reflecting the address (or other details) provided to the Company;
- Data availability and content can vary by country, some being more or less contemporaneous than others

## 5.7 Politically Exposed Persons

A PEP is defined as “an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person”.

PEP status itself does not incriminate an individual or entity. It does, however, put the applicant or an existing customer, or a beneficial owner, into a higher risk category.

Where, as a result of information identified by the Company’s third party systems, information suggests that an applicant, existing customer, or a beneficiary is a PEP, this should immediately be reported to the MLRO for EDD purposes:

- The MLRO will cause any necessary additional due diligence to be conducted, in order to:
  - Assess the money laundering risk
  - Determine whether it is appropriate to continue with the PEP relationship
- The assessment will include scrutiny of the relevant person’s personal circumstances or change in status, as well as any identifiable complexity or structuring of the business relationship (e.g. involving companies, trusts or foreign jurisdictions), to ensure clarity about and legitimacy of any transaction(s).
- Although, by definition, an individual might cease to be a PEP after having left office for one year, a risk-based assessment is still required when determining

whether appropriate monitoring of transactions or activity should continue to be applied at the end of this period. A longer period might be appropriate in order to ensure that the higher risks associated with an individual's previous position have adequately abated.

**Having due regard to EDD findings and the need for on-going monitoring arrangements, prior to any Compliance approval of a PEP relationship:**

- Approval should be obtained from the MLRO (or other senior manager) to establish (or continue) a customer relationship with a newly identified PEP
- Adequate steps should to taken establish the source of wealth and source of funding to be involved in the customer relationship or transaction
- The MLRO should ensure appropriate planning for conducting enhanced on-going monitoring if such a higher risk customer relationship is entered into, or continued

**Where, a decision is made to continue with a PEP relationship the reasoning must be documented by Compliance; and the MLRO should liaise with the business, to establish the:**

- Nature and extent of information and on-going monitoring that should be captured and applied to the customer relationship; and
- Duration and frequency of monitoring required.

**Where, a decision is made to decline a new application, or to discontinue an existing customer relationship, the MLRO will liaise with the business, to ensure that:**

- Identifiable money laundering risk is assessed and dealt with appropriately (e.g. funds received, or to be received, or to be refunded/paid away)
- Appropriate steps are taken to exit the customer relationship
- The customer is treated fairly and without prejudice to the firm's position

## 5.8 Nature of business

Particularly with regards to corporate customers, but the principle applies also to non-business customers, sufficient information should be obtained and recorded, to provide a clear understanding of the applicant's nature of business. This will enable an assessment to be made of whether the purpose for which an account is wanting be established (see below), is consistent with the type of business being (or to be) transacted.

Understanding the customer's business enables opportunities to be identified for the Company to offer to provide a broader range of relevant services, as well as,

understanding the customer's operational requirements for money transmission services.

## 5.9 Purpose of account

During a new applicant registration process information should also be obtained, which reflects a good understanding of the intended use of Company's services and enables an assessment to be made of the money laundering risk. This applies to both individuals and companies. Additional information sought and details to be recorded against customer records, might include some of the following:

**For personal accounts**

- A description of the customer's nature of employment
- Details of current address and any recent change of address during the past 12 months
- Expected source/origin of initial funds to be used in the account relationship (e.g. from a personal account in the customer's name)
- The source/destination of future funds
- Whether the source/ use of funds will remain the same during the course of the next 12 months, 2 years, etc.
- The anticipated transaction volumes, values and level of activity to be expected

**For business accounts**

- Intended use of account and how this links to customer's business.
- Expected source/origin of initial funds to be used in the account relationship (e.g. from a company/business account in the customer's name)
- Whether the initial source/intended use of funds will remain the same during the course of the next 12 months, 2 years
- The anticipated transaction volumes, values and level of activity to be expected

Recording the above information is a useful mechanism with which to aid deter and detect potential criminality, as well as providing a backdrop against which anomalies can be identified and/or account monitoring applied.

## 5.10 Red-flags

Where a customer appears reluctant to provide information or is otherwise evasive in his answers, this may be indicative of concerns about commercially sensitive information, or a red-flag to indicate money laundering risk. Where a doubt exists about information provided by a customer, or a concern is identified about lack of information, employees should contact Compliance for advice.

**These are generic examples of potential Red-flags that could be highlighted within the industry as a whole:**

- Attempts to obscure or avoid identifying detail of beneficial owners
- Unwillingness to disclose the requested information
- Customers whose lavish lifestyle appears to exceed known sources of income
- Frequent changes to shareholders or Partners
- Excessive or unnecessary use of nominees
- Unnecessary granting of power of attorney
- The involvement of companies in a transaction for no obvious commercial purpose
- Subsidiaries having no apparent purpose
- Uneconomic or inefficient structuring of transaction for no obvious commercial purpose, or which might be used by group structures for tax evasion purposes
- Unusual, or out of the ordinary instructions
- Repetitive or inexplicable changes to instructions
- Use of bank accounts or funds transfers in several currencies without reason
- Transfers of funds without evidence of underlying transactions
- Sums paid exceed supporting information provided about goods/service costs
- Customers appear disinterested in reducing commissions, exchange rate cost, etc.
- Higher than expected funds transfer arrangements when considering the typical values and volumes expected of such customers
- Corporate customers transferring large sums of money to or from overseas locations having no apparent link to the customer's nature of business

- Customers paying round sum amounts to numerous bank accounts, or in round sum international transfer
- Unexplained transfers of significant sums through several bank accounts

In any instance where money laundering is suspected, details should immediately be notified to the MLRO, without alerting the customer or other person about whom a suspicion is held.

### 5.11 Capturing information

When deciding whether or not to approve a new customer application, or when responding to queries about an existing customer, Compliance should make an informed decision. It is important therefore, for employees having information relevant to a customer, or a customer's account, that the information content is available to the Compliance team.

**The following documents and records should be retained in accordance with procedures for Record Keeping, set out below:**

- Telephone notes of discussions with customers
- Correspondence or other documentation received from customers
- Correspondence or other documentation received about customers

# 6 Identification requirements - new applicants

## 6.1 Private individuals

**The following information must be obtained for all applicants who are private individuals:**

- Full name
- Current residential address
- Date of birth

For an individual's identity to be verified electronically: electronic checking should use the person's full name, address and date of birth as a basis.

**To confirm identity, the standard level of confirmation required, is:**

- One match on an individual's full name and current residential address, **and**

- A second match on the full name and **either** his current address **or** his date of birth.

A standard electronic confirmation of identity is likely to apply to most applicants or customers who are private individuals; except where:

- Electronic verification is not possible or practicable.
- An applicant (or an existing customer) is determined to be a PEP.

Where electronic verification is not appropriate, evidence to verify identity can take a number of forms. For a private individual reliance will be placed on an identity document, such as, a passport, photo-card driving licence or some other valid Government issued photo ID Card.

If identity is to be verified from documents, this should be based on:

**either a government-issued[2] document which incorporates:**

- the customer's full name and photograph, and
  - either his residential address
  - or his date of birth.

**or** a government-issued document (without a photograph) which incorporates the customer's full name, **supported by** a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, a regulated utility company, or an FCA-regulated firm in the UK financial services sector, or in an equivalent jurisdiction, which incorporates:

- the customer's full name and
  - either his residential address
  - or his date of birth

The section below headed 'Identification Documents' identifies typical documentary evidence that is considered acceptable when seeking to confirm identity. In normal circumstances, the applicant should be asked to supply two items of identity verification and adopting the risk based approach, there may be a requirement for the documents to be endorsed by an Appropriate Person.

Company's minimum standard for an acceptable certified copy of an original document is one where: the endorsing party is someone independent of the client and who ordinarilyholds a responsible position.

[2] Issued by a central government department or by a local government authority or body

## 6.2 Private (or unlisted) company

Before entering into a business relationship with a private (or unlisted) company and / or those who represent it, appropriate verification checks must be applied where impersonation fraud may be a risk; particularly where the identity of those who represent the company is not verified face-to-face.

Steps must be taken to be reasonably satisfied that the person the Company deals with is properly authorised by the applicant (e.g. by way of a written authority addressed to the Company which is signed by the Partners issued on company letter head).

Where an entity is known or believed to be linked to a PEP (perhaps through a Partnership or shareholding), or to a jurisdiction assessed as carrying a higher money laundering or terrorist financing risk, it is likely that this will put the entity into a higher risk category and EDD should be applied.

It is important that Company's records in relation to a private company applicant, enable it to reflect an understanding of the company's legal and ownership structure, and that sufficient additional information has been obtained on the nature of the company's business, and the reasons for seeking Company's services.

**For company applicants, the Company must:**

- Take reasonable steps to understand ownership and control of the customer. Information may need to be obtained from the Company Secretary or the Partners. Alternatively, the most recent audited accounts filed with the Company Registry might provide sufficient detail about a company's operations, business activities and ownership structure
- Obtain reliable information and assess the money laundering and terrorist financing risk associated with an applicant, the customer and business relationship; as well as the services sought and/or the transactions involved

## 6.3 Standard Evidence

**The following information must be obtained for all private company applicants:**

- Full name
- Registered number
- Registered office in country of incorporation
- Business address

**Plus:**

**Either** A private company does not usually qualify for SDD. Under a risk-based

approach, however, provided that confirmation is provided in writing by a reliable and independent source, the imposition of, say, regulatory obligations on an applicant firm (or customer) which is a private company, might be considered to provide an equivalent level of confidence in the company's public accountability.

Therefore, evidence that a corporate customer is subject to licensing and prudential regulatory regime of a statutory regulator in the EU (e.g. FCA, OFGEM, OFWAT, OFCOM or an equivalent jurisdiction), may be sufficient to satisfy identity verification requirements of such a customer.

**Or For all private or unlisted companies where SDD cannot be applied:**

- The company's existence should be verified from:
  - either confirmation of the company's listing on a regulated market
  - or a search of the relevant company registry
  - or a copy of the company's Certificate of Incorporation
- The following information must also be obtained:
  - Names of all Partners
  - Names of beneficial owners who hold or control over 25% of the shares or voting rights or otherwise exercise control over the management of the company

Where electronic verification is not possible (for either corporate or personal identity verification) and reliance is to be placed on documentation supplied by an applicant (see also: Identification Documentation, page):

- Consideration should be given to whether any of the documents are forged
- If they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity

## 6.4 Partners

Following assessment of the money laundering or terrorist financing risk presented by a customer company, it may be appropriate to verify the identity of one or more Partners, as appropriate, in accordance with the principles for private individuals (i.e. see 5.1 above).

**In that event:**

- Verification is likely to be appropriate for those who have authority to operate an account or to give Company instructions concerning the use or

transfer of funds, but might be waived for other Partners

- A requirement may already exist to identify director(s) as beneficial owner(s) if they own or control more than 25% of the company's shares or voting rights

## 6.5 Beneficial owners

**In the case of a body corporate a beneficial owner includes any individual who:**

- As respects anybody other than a company listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body;

or

- As respects anybody corporate, otherwise exercises control over the management of the body

As part of collecting standard evidence, details of all individual beneficial owners owning or controlling more than 25% of the applicant company's shares or voting rights, even where these interests are held indirectly will be sought.

**Verification requirements differ between a customer and a beneficial owner:**

- Customer identity must be verified on the basis of documents, data or information obtained from a reliable and independent source
- The obligation to verify beneficial owner identity is based on the Company taking risk-based and adequate measures, to be satisfied that it knows who the beneficial owner is

In reviewing information obtained about a company's beneficial ownership, Compliance will determine whether a need exists to seek further information about one or more beneficial owners; for example, whether to use records of beneficial owners in the public domain (if any), to arrange further contact with customers to seek relevant data, or to obtain the information otherwise.

## 6.6 Mandate signatories

For operational purposes, a list is likely to be maintained of those authorised to give instructions (on behalf of the company) for the movement of funds, along with an appropriate instrument authorising one or more Partners (or equivalent) to give the firm such instructions.

Where the identity of relevant company Partners has been verified, the identities of individual signatories need only be verified on a risk-based approach. If, for example,

all payment instructions are expected to originate from a customer's in-house accountant, who is not the Finance Director, a risk-based approach might be to verify the Accountant's identity.

**It will be ensured that:**

- Standard evidence has been obtained and documented.
- Company identity has been reliably verified, either electronically or via reference to reliable source documents.
- The identity of appropriate Partners and other company individuals has been verified.
- Signatories and representatives dealing with the Company on behalf of thecompany have been properly authorised by the company.
- Shareholders with a beneficial interest of greater than 25% have been confirmed and their identity verified.
- Details of the client's 'nature of business and 'purpose of account' has been recorded.

## 6.7 Companies listed on regulated markets

The Company is not required to verify the identity of a corporate customer whose securities are listed on a regulated EEA market or equivalent overseas, which is subject to specified disclosure obligations.

This is due to the fact that such companies are publicly owned and generally accountable.

The exemption also applies to companies that are majority-owned and consolidated subsidiaries of such companies.

If the market is outside the EEA, but is one which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligation in the EU, similar treatment is permitted.

For companies listed outside the EEA on markets which do not qualify for SDD, the standard verification requirement for private and unlisted companies should be applied.

The European Commission maintains a list of regulated markets within the EU at ec.europa.eu/internal_market/securities/isd/mifid_en.htm.

## 6.8 Other customer types

The majority of Company's customers are expected to be individuals from Asia, South America and MENA who will use the Company's platform for speculating on financial markets. It is unlikely that any of the customer types detailed below will arise, but forcompleteness these are included in this policy. This section of Guidance provides an overview of these customer types and their respective identification requirements.

## 6.9 Trusts

*(See also JMLSG Guidance 5.3.244ff)*

In some trusts and similar arrangements, instead of being an individual, the beneficial owner is a class of persons who may benefit from the trust. Where only a class of persons is required to be identified, it is sufficient to ascertain and name the scope of the class. It is not necessary to identify every individual member of the class.

For trusts or foundations that have no legal personality, those trustees (or equivalent) who enter into the business relationship with the Company, in their capacity as trustees of the particular trust or foundation, are customers on whom the Company must carry out full CDD measures. Following a risk-based approach, in the case of a large, well knownand accountable organisation, the Company may limit the trustees considered customers to those who instruct the Company. Other trustees will be verified as beneficial owners.

**The beneficial owner of a trust is defined by reference to three categories of individual:**

- Any individual who is entitled to a specified interest (that is, a vested, not a contingent, interest) in at least 25% of the capital of the trust property
- As respects any trust other than one which is set up or operates entirely for the benefit of individuals with such specified interests, the class of persons in whose main interest the trust is set up or operates
- Any individual who has control over the trust

The trustees of a trust will be beneficial owners, as they will exercise control over the trust property. In exceptional cases, another individual may exercise control, such as a trust protector, or a settlor who retains significant powers over the trust property. For the vast majority of trusts, either there will be clearly identified beneficiaries (who are beneficial owners within the meaning of the MLR), or a class of beneficiaries. These persons will be self-evident from a review of the trust's constitution. In the case of a legal arrangement that is not a trust, the beneficial owner means

- Where the individuals who benefit from the entity or arrangement have been

determined, any individual who benefits from at least 25% of the property of the entity or arrangement;

- Where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interest the entity or arrangement is set up or operates;

Any individual who exercise control over at least 25% of the property of the entity or arrangement

**Details to be recorded and maintained:**

**Obtain the following:**

- Full name of Trust
- Nature and purpose of Trust (e.g. discretionary, testamentary, bare)
- Country of establishment
- Names of all trustees
- Names of any beneficial owners
- Name and address of any protector or controller

Documentary evidence required to verify legal purpose: Scheme Trust Deed or latest Deed of Appointment, listing all current Trustees.

Additional: Names, addresses and dates of birth and identity verification required for trustees in whose names an investment is registered (i.e. if trustee is a private individual, personal identity and address verification also required).

Names and confirmation of the identity of any other trustees, names and addresses and confirmation of the identity of any protector or controller, plus names and confirmation of identity of any nominated beneficiaries having an interest of at least 25%.

Identification for any third party payers

## 6.10 Partnership/unincorporated body

*(see also JMLSG 5.3.162)*

Partnerships and unincorporated businesses, although principally operated by individuals, or groups of individuals, are different from private individuals in that there is an underlying business. This business is likely to have a different money laundering or terrorist financing risk profile from that of an individual.

The beneficial owner of a partnership is any individual who ultimately is entitled to

or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership, or more than 25% of the voting rights in the partnership, or who otherwise exercise control over the management of the partnership.

In verifying the identity of such customers, primarily have regard to the number of partner/principals. Where these are relatively few, the customer should be treated as a collection of private individuals, and identified accordingly.

Where numbers are larger, decide whether to regard the customer as a collection of private individuals, or whether it might be appropriate to be satisfied with evidence of membership

of a relevant professional or trade association. In either circumstance, there is likely to be a need to see the partnership deed (or other evidence in the case of sole traders or other unincorporated businesses), to be satisfied that the entity exists, unless an entry in an appropriate national register may be checked.

**Details to be recorded and maintained:**

**Obtain the following:**

- Business address
- Names of all partners/principals who exercise control over the management of the partnership
- Names of individuals who own or control over 25% of its capital or profit, or of its voting rights

Documentary evidence required to verify legal purpose: Partnership deed showing rights and duties of the partners.

Additional: Name, address, date of birth and identity verification is required for partners or owners in whose names investments are registered (i.e. for private individuals, personal identity and address verification is required).

## 6.11 Charities

*(see also JMLSG 5.3.224)*

**Details to be recorded and maintained:**

**Obtain the following:**

- Nature of body's activities and objects
- Names of all trustees (or equivalent)

- Names or classes of beneficiaries

Documentary evidence required to verify legal purpose: Charities have their status because of their purposes, and can take a number of legal forms. Some may be companies limited by guarantee, or incorporated by Royal Charter or by Act of Parliament; some may take the form of trusts; others may be unincorporated associations.

Names, addresses, dates of birth and identity verification required for the trustees/ officers in whose names investments are registered. Trustees/Officers should have appropriate authority to operate an account or give instructions to Pearl concerning the use or transfer of funds or assets (for private individuals, personal identity and address verification is required). Additional: Confirmation of the identity of all other officers/trustees (i.e. Name, address and dates of birth); this can be achieved by one of the verified partners or proprietors providing an original signed letter on the customer's letterhead, incorporating a listing of relevant persons (i.e. other officers).

# 7 Identification documentation

## 7.1 Verifying identity Using documentation

In circumstances where on-line verification of client identity is not possible, the Company will adopt the following approach to the documentary identity verification required.

Countries will be assessed using a risk based approach and the requirements for documentary identity verification will become more stringent as the perceived risk of the jurisdiction increases.

**Countries will be classified as follows:**

**Low Risk:** **EEA Countries**

**Medium Risk:** **FATF Countries**

**Higher Risk:** **All other Territories**

**Highest Risk:** **FATF, High Risk, HMT High Risk Jurisdictions**

Company's Compliance Department will keep an up to date list of the category of each jurisdiction of the world.

**Document Requirements:**

**Low Risk:** **One item list 1, plus one item list 2**

**Medium Risk:** One item list 1, plus two items list 2

**Higher Risk:** One item list 1, plus one item list 2 (certified see 7.2)

**Highest Risk:** Two items list 1, plus one item list 2 (financial statement only) (certified see 7.2)

**Sanctioned Countries:** Business will be Rejected

**LIST 1**

- Unexpired passport
- Unexpired photocard driving licence
- National Identity card
- Firearms certificate or shotgun licence issued by a Police authority
- Other unexpired Government issued photo ID card

**LIST 2**

- Council tax bill / demand letter*
- Notification of entitlement to state / local authority benefit *
- Notification of entitlement to educational loan / grant *
- Notification of entitlement to other government / local authority grant *
- Bank statement (not internet printed) **
- Credit card statement (not internet printed) **
- UCAS letter (student's only) *
- Local council rent card or tenancy agreement *
- Official revenue correspondence (Inland Revenue) correspondence including name, address & permanent NI number *
- Pension / benefit correspondence *
- Utility bill (not mobile phone, satellite / cable TV or internet printed bills) **
- Confirmation from work / school / college / university / care institution confirming name, address and details of employment / student / residence status (students only) *
- Disclosure certificate issued by appropriate UK Agency, in the last 12 months. (UK Citizens only)

* Must be the most recently issued document and less than 12 months old

** Must be the most recently issued document and less than 3 months old (except water bills – less than 12 months old)

## 7.2 Appropriate persons

Where a client is dealt with remotely (i.e. non face-to-face) adequate measures must be taken to compensate for the higher risk of identity theft/fraud, impersonation and money laundering.

Where identity is verified by reference to copy documents supplied by a client, additional verification checks should be deployed to manage the risk of impersonation fraud. Such additional check may consist of robust anti-fraud checks undertaken as part of existing procedure, or may include, for example, requiring copy documents to be certified by an appropriate person.

The Glossary of Terms in JMLSG guidance identifies 'appropriate person', as: Someone in a position of responsibility who knows, and is known by a client, and may reasonably confirm the client's identity.

---

Company's minimum standard for an acceptable certified copy of an original documentis one where: the endorsing party is someone independent of the client and who ordinarily holds a responsible position.

The independent person should confirm in (clearly legible) handwriting and by personal signature on the copy document that, he/she has:

**(a)** Seen the original of the endorsed copy document; **and**

(b) Known the client (whose identity is being verified) for at least two years.

---

An individual whose personal endorsement (as above) on a client's copy documents, is acceptable when at the time of providing such endorsement, the person holds or carries out one of the following professions/offices:

- Articled clerk of a limited company
- Assurance agent of recognised company
- Bank/building society official
- Chairman/director of a UK incorporated entity
- Chartered accountant
- Civil servant (permanent)
- Commissioner of Oaths
- Councillor: local or county

- Director or manager of a VAT registered firm/entity
- Director, manager or personnel officer of a VAT registered firm/entity
- Doctor, Surgeon, Dentist or Veterinary
- FCA regulated IFA / Broker
- HMRC Regulated MSB, High Value Dealer
- Insurance agent (full time) of a recognised company
- Local government officer
- Manager, personnel officer (of incorporated company/partnership)
- Member of Parliament
- Member of the Bar Council
- Member of the Judiciary, Justice of the Peace or Court Clerk
- Minister / member of clergy in a well-known and recognised religion
- Officer of the UK armed services (active or retired)
- OFT Regulated Estate Agent
- Person with honours (e.g. OBE, MBE etc.)
- Police Officer, H & M Revenue & Customs
- Post Office official
- Social worker
- Solicitor in practice
- Teacher, lecturer at accredited institution
- Trade union officer
- Warrant officers and Chief Petty Officer

# 8 Monitoring

Information collected from (or about) applicants who subsequently become customers, must, as far as reasonably practicable, be kept up to date. Information obtained at customer take-on, or when monitoring for variances against that initial customer profile, is a useful mechanism with which to aid deter and detect potential criminality.

Once identity is satisfactorily verified, there is usually no need to re-verify identity, unless:

- Subsequent doubts arise as to the veracity or adequacy of evidence previously obtained for the purposes of customer identification
- The customer changes name (e.g. through marriage or deed-poll for a private individual, or by changing company name, for a legal entity)
- Beneficial ownership or control changes materially to that which was understood and documented at customer take-on
- As new/emerging risk dictates

With regards to the nature and purpose of activity transacted, to ensure that on-going monitoring/risk-assessment of customer transactions is fit-for-purpose, appropriate measures should be taken to maintain up-to-date information about customers; whether on a routine or event driven basis.

## 8.1 Regular risk-assessments and refresh

Risk based reviews are undertaken on existing relationships at predetermined trigger events, such as:

**Out-of-the-ordinary account activity**

- An existing customer applying to open a new account or establish a new relationship
- An existing customer applying to open a new account or establish a new relationship
- Change in ownership or control of a customer entity, or change of business, operating or contact address
- Change of standing data for personal customers, such as, residential or contact address
- Adverse media reporting about a customer or customer business
- Transactions with different territories/jurisdictions, particularly higher-risk countries
- Account inactivity or dormancy for a defined period
- Other criteria developed by Compliance

A suspicious transaction or suspicious circumstances may arise at any time during a relationship with a client. Be on the lookout for any activity which is inconsistent with

the client's expected and legitimate transactions:

- Unusually large deposits – outside the normal trends of the account operation
- Requests to deposit cash
- Attempted use of third parties for deposits/withdrawals
- Payments to/from high risk countries
- Difficulties in obtaining ID documentation
- Transactions with no apparent purpose
- Funding an account but not trading and then withdrawing the funds or when a client enters into a business relationship with the Company for a single transaction or for a very short period of time only
- Unusual transactions - activity that is inconsistent or out of the ordinary range of a particular client's usual trading pattern
- For corporate accounts, does the legal and corporate structure, its ownership and control, make sense?
- Has the customer suggested changes to our procedures in order to avoid providing certain information?

**Other things to look out for:**

- Sudden, substantial increases in cash deposits or levels of investment without adequate explanation
- Large electronic transfers in and out of the account
- Reactivation of dormant accounts
- No known source of income or activity inconsistent with a stated occupation
- Frequent address changes

The above lists of possible suspicious activities are non-exhaustive and if you think that the activities of a client seem unusual or if you have any suspicions, it should be reported to the MLRO.

Transactions undertaken on client trading accounts will be monitored as part of the Company's risk management strategy. Any transactions which are deemed abnormal or suspicious are reported to the MLRO.

As part of the regular compliance monitoring initiative, the compliance department will undertake a monthly review of compliance with anti-money laundering regulations. A monthly review of KYC documentation will take place. Each month, a random sample of new accounts will be checked to ensure compliance with internal policy and procedures.

Senior management will be informed of the results of this monitoring during the monthly board meetings.

## 8.2 Due Diligence on Third Party Relationships

It is essential that firms understand who they working with when establishing business relationships and in doing this firms are expected to:

- Establish and document policies with a clear definition of a 'third party' and the due diligence required when establishing and reviewing third party relationships.
- Have more robust due diligence on third parties which pose the greatest risk of bribery and corruption, including a detailed understanding of the business case for Using them.
- Have a clear understanding of the roles clients, and third party suppliers, such as solicitors undertake in transactions to ensure they are not carrying out higher risk activities.
- Take reasonable steps to verify the information provided by third parties during the due diligence process.
- Use third party forms which ask relevant questions and clearly state which fields are mandatory.
- Have third party account opening forms reviewed and approved by compliance, risk or committees involving these areas.
- Use commercially-available intelligence tools, databases and/or other research techniques such as internet search engines to check third party declarations about connections to public officials, and other parties.
- Routinely inform all parties involved in the transaction about the involvement of third parties being paid commission.
- Ensure current third party due diligence standards are appropriate when business is acquired that is higher risk than existing business.
- Consider the level of bribery and corruption risk posed by a third party when agreeing the level of commission.

- Set commission limits or guidelines which take into account risk factors related to the role of the third party, the country involved and the class of business.
- Pay commission to third parties on a one-off fee basis where their role is pure introduction.
- Take reasonable steps to ensure that bank accounts used by third parties to receive payments are, in fact, controlled by the third party for which the payment is meant. For example, broker firms might wish to see the third party's bank statement or have the third party write them a low value cheque.
- Apply higher or extra levels of approval for high risk third party relationships.
- Regularly review third party relationships to identify the nature and risk profile of third party relationships.
- Maintain accurate central records of approved third parties, the due diligence conducted on the relationship and evidence of periodic reviews.

## 8.3 Payment Controls

**Firms must consider the implications of the Act in conjunction with payments, commission and fees it pays by:**

- Ensuring adequate due diligence and approval of third party relationships before payments are made to the third party.
- Risk-based approval procedures for payments and a clear understanding of why payments are made.
- Checking third party payments individually prior to approval, to ensure consistency with the business case for that account.
- Regular and thorough monitoring of third party payments to check, for example, whether a payment is unusual in the context of previous similar payments.
- A healthily sceptical approach to approving third party payments.
- Adequate due diligence on new suppliers being added to the Accounts Payable system.
- Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced.
- Limiting third party payments from Accounts Payable to reimbursements

of genuine business-related costs or reasonable entertainment.

- Ensuring the reasons for third party payments via Accounts Payable are clearly documented and appropriately approved.
- The facility to produce accurate MI to facilitate effective payment monitoring.

## 8.4 Staff Recruitment and Vetting

**When new or existing staffs are appointed to new roles the firm has an obligation to:**

- Vet staff on a risk-based approach, taking into account financial crime risk.
- Enhance vetting – including checks of credit records, criminal records, financial sanctions lists, commercially available intelligence databases and the CIFAS Staff Fraud Database – for staff in roles with higher bribery and corruption risk.
- Apply risk-based approach to dealing with adverse information raised by vetting checks, taking into account its seriousness and relevance in the context of the individual's role or proposed role.
- Ensure that where employment agencies are used to recruit staff in higher risk positions, having a clear understanding of the checks they carry out on prospective staff.
- Conduct periodic checks to ensure that agencies are complying with agreed vetting standards.
- Apply a formal process for identifying changes in existing employees' financial soundness which might make them more vulnerable to becoming involved in or committing corrupt practices.

## 8.5 Training and Awareness

**Firms must ensure that they:**

- Provide good quality, standard training on anti-bribery and corruption for all staff.
- Have additional anti-bribery and corruption training for staff in higher risk positions.
- Ensure staffs responsible for training others have adequate training themselves.
- Ensure training covers practical examples of risk and how to comply with policies.

- Test staff understanding and using the results to assess individual training needs and the overall quality of the training.
- The staff records setting out what training was completed and when.
- Provide refresher training and ensuring it is kept up-to-date.

## 8.6 Risks from Remuneration Structures

**All firms should consider whether to:**

- Assess remuneration structures give rise to increased risk of bribery and corruption.
- Determine individual bonus awards on the basis of several factors, including a good standard of compliance, not just the amount of income generated.
- Defer and claw back provisions for bonuses paid to staff in higher risk positions.

# 9 Record keeping

## 9.1 Adequate records

The firm, having considered the regulations, insist appropriate records concerning customer identification and transactions must be maintained, as evidence of work undertaken in complying with any legal and regulatory obligations, as well as for use as evidence in any investigation conducted by a law enforcement agency or regulatory body.

Reasonable care must be taken to make and keep adequate records appropriate to the scale, nature and complexity of business undertaken with customers, covering:

- Customer information
- Transactions
- Internal and external suspicion reports
- Information not acted upon
- MLRO annual (and other) reports
- Training (and information about the effectiveness of training)
- Compliance monitoring

## 9.2 Customer information

With regard to customer information, records to be retained are:

- A copy of, or the references to, the evidence of customer identity obtained when: establishing (or updating) details held about a customer; monitoring the business relationship; or when performing enhanced due diligence ('customer records');
- The supporting records (consisting of the original documents or appropriate copies) in respect of business relationships or occasional transactions which are the subject of customer due diligence measures or on-going monitoring ('customer supporting records').

# 10 Breaches of Anti-Money Laundering Policy

Any breaches of the Anti-Money Laundering rules will be recorded on The Firm's breach log in conjunction with its Regulatory Breach policy.

# Appendix 1 - Use of electronic identification checks

For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source ( e.g., a single check against the Electoral Roll) is not normally enough on its own to verify identity.

Verifying a legal entity's name and identity by way of electronic verification is possible where the relevant company registry data is accessible on-line, or via a reputable third party service provider.

Checks may be carried out directly by a PSP, or via one or more commercial service providers, such as, GB Group, C6, Equifax, Experian, or World-Check, or others.

Information supplied by the relevant provider(s) should be sufficiently extensive, reliable and accurate.

**Some of the typical parameters to consider when assessing a service provider include:**

- Cost and methodology (e.g. in-house, out-sourced, etc.)
- Responsiveness
- Registration with the Information Commissioners Office to store personal data
- Uses a range of positive information sources that can be called upon (if required to do so) to link a customer to both current and previous circumstances
- Accesses negative information sources, such as, databases relating to identity fraud and deceased persons
- Accesses a wide range of alert data sources (e.g. sanctions lists, news media, etc.)
- Operate processes which enable a user-firm to know what checks were carried out, the results of those checks, and a rating for how much certainty they give as to the identity of the subject
- Processes that allow an enquirer to capture and store the information they used to check and verify an identity

# Appendix 2 - Notification to Nominated Officer of Suspicious Activity

## Form A

| **Client and Activity Details** | |
|---|---|
| Client Name: | |
| Client Account Number: | |
| Client Address: | |
| | |
| Grounds for Suspicion: | |
| | |
| | |
| | |
| | |
| Date and Time of Activity: | |
| What Follow-Up is Required for the Client? | |

| **Employee Details:** | |
|---|---|
| Your Name: | |
| Your Signature: | |
| Date of report: | |
| Nominated Officer signature[3]: | |

[3] You should receive a copy of the completed form with the Nominated Officers' signature as proof of receipt.