

|  |
| --- |
| Firms Logo |
| Anti Money Laundering & Counter Terrorist Financing Policy |
| [Type the document subtitle] |
|  |
|  |
| **[Pick the date]** |

Amendments to this Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Status** | **Date** | **Amendment Comments** | **By Whom** |
| 0.1.0.00 | Draft | December 2014 | Initial draft | Compliance Consultant |
| 0.2.0.00 | Draft | May 2016 | Draft | Compliance Consultant |
| 0.3.0.00 | Draft | May 2017 | Draft | Compliance Consultant |
| 0.4.0.00 | Draft | June 2017 | Draft | Compliance Consultant |
| 0.4.1.00 | Draft | January 2018 | Fully MLR 2017 updated and reviewed | Compliance Consultant |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

From time to time this policy will be updated to reflect changes to {NAME\_OF\_FIRM\_SHORT}’s regulated business or changes to the regulations to which {NAME\_OF\_FIRM\_SHORT} is subject. The Compliance Officer will ensure that all appropriate amendments are made to this manual, and this will be overseen by the Compliance Director. The dates of the amendments are recorded below. Please ensure that you have the most up-to-date version of this manual by confirming the correct version number with Compliance.

**Table of Contents**

**\* READ THIS NOW \* READ THIS NOW \* READ THIS NOW \* READ THIS NOW \***

Amend the detail on this page as required then delete this section. Use “Find & Replace” in your word processor software.

**Variable for personalisation** {Name\_of\_Firm} Replace with your firm’s name

{NOFMLRO} Replace with your Firms MLRO name

“AML & CTF Manual 20xx” replace

If any section of this manual is not required, simply cut the section completely and then update the Table of Contents.

If any section requires amendment, addition or subtraction of text, make sure you update the Table of Contents on completion.

This manual is not maintained by Compliance Consultant and before adopting it or approving it as fit for purpose we would recommend that you review the entire document from a legal and compliance aspect. We have completed it as best we can from current legislation and guidance from the FCA’s FC1 & FC2, in accordance with the Money Laundering Regulations 2017 and JMLSG Guidance and it was correct at time of writing.

[Amendments to this Policy 3](#_Toc503541380)

[1 CHAPTER 1: INTRODUCTION 5](#_Toc503541381)

[2 CHAPTER 2: OFFENCES 8](#_Toc503541382)

[3 CHAPTER 3: INTERNAL COMMUNICATIONS 13](#_Toc503541383)

[4 CHAPTER 4: THE RISK BASED APPROACH 15](#_Toc503541384)

[5 CHAPTER 5: CUSTOMER DUE DILIGENCE PROCEDURE 19](#_Toc503541385)

[6 CHAPTER 6: IDENTIFICATION EVIDENCE 26](#_Toc503541386)

[7 CHAPTER 7: INTRODUCTIONS BY INTERMEDIARIES 35](#_Toc503541387)

[8 CHAPTER 8: SUSPICIOUS TRANSACTIONS 37](#_Toc503541388)

[9 CHAPTER 9: TRAINING AND AWARENESS 41](#_Toc503541389)

[10 CHAPTER 10: MONITORING 42](#_Toc503541390)

[11 CHAPTER 11: RECORD RETENTION 44](#_Toc503541391)

[Appendix 1: Suspicious Transaction/Activity Reporting Form (Money Laundering) 47](#_Toc503541392)

[Appendix 2: Register of Attendees 51](#_Toc503541393)

[Appendix 3: New Account Opening Form (“NAO”) *[Amend as required]* 52](#_Toc503541394)

[Appendix 4: Documents for Individuals 71](#_Toc503541395)

[Appendix 5: Useful Information Sources 72](#_Toc503541396)

[Appendix 6: Anti-Money Laundering Handbook Declaration 74](#_Toc503541397)

[Appendix 7: Post-Transaction Review Form 75](#_Toc503541398)

[Appendix 8: Transparency International Corruption Perception Index (http://www.transparency.org/) 76](#_Toc503541399)

[Appendix 9: PEP Questionnaire: Identification of Politically Exposed Persons (PEP’s) 84](#_Toc503541400)

[Appendix 10: Beneficial Owner Declaration 85](#_Toc503541401)

[Appendix 11 Useful Links 87](#_Toc503541402)

**To update** – simply right click in field, “update field”, select “entire table” or “page numbers” only.

# CHAPTER 1: INTRODUCTION

## {NAME\_OF\_FIRM\_LONG} Anti-Money Laundering & Counter Terrorist Financing Policy

## {NAME\_OF\_FIRM\_LONG} (“{NAME\_OF\_FIRM\_SHORT}”) is committed to maintaining effective prevention and detection measures to assist the law enforcement authorities in combating financial crime. This handbook sets out the policies and procedures which have been adopted to meet {NAME\_OF\_FIRM\_SHORT} ’s legal obligations under the UK’s anti-money laundering and counter terrorist legislation.

## These policies and procedures must be adhered to at all times.

## {NAME\_OF\_FIRM\_SHORT} seeks to ensure at all times that:

## Clients’ identities are satisfactorily verified in accordance with the firm’s risk based approach before {NAME\_OF\_FIRM\_SHORT} does business with them

## {NAME\_OF\_FIRM\_SHORT} knows its clients and understands their reasons for doing business with us both at the client acceptance stage and throughout the business relationship

## Our staff are trained and made aware of both their personal legal obligations and the legal obligations of {NAME\_OF\_FIRM\_SHORT}.

## Our staff are trained to be vigilant for activities where there are reasonable grounds for suspicion that money laundering could be taking place and to make the reports to the MLRO.

## Sufficient records are kept for the required period.

## We establish, maintain and implement appropriate procedures to achieve these objectives

## Money laundering, fraud and market abuse threats are dynamic, and criminals constantly devise new techniques and exploit the easiest targets in the financial services sector. To mitigate the risk of being used as a vehicle for financial crime {NAME\_OF\_FIRM\_SHORT} will systematically assess, mitigate and monitor these risks. It will seek to identify fraud, money laundering and market abuse as well as conduct risk implications at an early stage of the client acceptance process, escalate this to senior management and take appropriate action.

## A risk based approach adopted by {NAME\_OF\_FIRM\_SHORT} is the driver of our overall strategy of fighting financial crime. Through this approach we identify the areas of greatest vulnerability and focus our resources on those areas. Ultimate responsibility for this approach lies with the senior management but all staff carry a responsibility to maintain the effectiveness of systems and controls.

## Given the nature of risks involved it is not possible to cover every possible eventuality in this handbook. Should an issue arise that is not specifically covered in this handbook, employees should refer to the MLRO for further guidance.

## Financial Crime Risk

FCA’s financial crime objective encompasses the prevention of financial fraud, market abuse and money laundering. Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds.

Money laundering and terrorist financing risks are closely related to the risks of fraud and insider dealing. While these are separate offences, money laundering involves handling the proceeds of any crime, including the proceeds of these activities.

The ability to launder the proceeds of crime through the financial system is vital to the success of criminal operations. London, as one of the world’s major financial centres, has a major role to play in combating money laundering. Firms that become involved in money laundering risk prosecution and damage to their reputation.

In recognition of this the procedures that {NAME\_OF\_FIRM\_SHORT} has adopted, to reduce the incidence of financial crime, focus on knowing our clients, understanding their businesses, carrying our proportionate verification checks and identifying and reporting suspicious activity.

## Law, Regulation and Industry Practice

{NAME\_OF\_FIRM\_SHORT} is subject to the provisions of the UK Money Laundering Regulations 2017 as well as the FCA Senior Management Arrangements Systems and Controls sourcebook. The Joint Money Laundering Steering Group guidance 2017 (“JMLSG”) (as amended) provides practical interpretation of legal and regulatory requirements and indicates good industry practice. {NAME\_OF\_FIRM\_SHORT} has taken account of the JMLSG when devising a risk-based approach to the prevention of money laundering risk. The latest details can be found at the website <http://www.jmlsg.org.uk/>.

## General Principles

In order to comply with the UK laws, regulations and guidance, {NAME\_OF\_FIRM\_SHORT} adopts the following principles:

### Anti-Money Laundering Policies

{NAME\_OF\_FIRM\_SHORT} has implemented policies, procedures and controls aimed at deterring criminals from using {NAME\_OF\_FIRM\_SHORT} for the laundering of proceeds of crime. These policies and procedures are tailored to the risk posed by individual clients, in accordance with the JMLSG.

### Money Laundering Reporting Officer

{NAME\_OF\_FIRM\_SHORT} has appointed {NOFMLRO} as its Money Laundering Reporting Officer (“MLRO”). The MLRO acts as the central point of contact both with the law enforcement agencies and internally, in relation to all matters relating to money laundering. The MLRO monitors {NAME\_OF\_FIRM\_SHORT}’s compliance with anti-money laundering procedures and submits reports to senior management at least on an annual basis. The MLRO is an approved person under the FCA’s Approved Persons regime.

### Customer Due Diligence (‘CDD’)

{NAME\_OF\_FIRM\_SHORT} has established Customer Due Diligence procedures to identify the users of its services and, in relation to higher-risk clients, the principal beneficial owners and origins of funds. These procedures include knowing the nature of our clients’ businesses and being alert to abnormal transactions.

### Suspicious Transactions

Unexplained or abnormal transactions or activities that are suspected of being linked to criminal activity should be reported to the MLRO in writing without delay using the Suspicious Transaction Reporting Form (Money Laundering) in Appendix 1. The MLRO will determine whether to report the suspicions to the National Crime Agency (“NCA”) (formerly Serious Organised Crime Agency – SOCA). If the MLRO is absent, reports should be made to the Deputy MLRO who is [Deputy\_MLRO\_Name]. An acknowledgment of receipt should be obtained from the MLRO for every such report.

### Training

All personnel must be informed of their individual and collective responsibilities and {NAME\_OF\_FIRM\_SHORT}’s anti-money laundering policies. Personnel are provided with training to enable them to understand the vulnerabilities of {NAME\_OF\_FIRM\_SHORT}’s business and to recognise and report suspicious activities.

### Record-Keeping

{NAME\_OF\_FIRM\_SHORT} keeps records of who has been trained and the timing and form of training sessions. We retain all records verifying the identity of our clients for at least 5 years following the end of the business relationship. We also retain the records of any internal reports of suspicion submitted to the MLRO and any disclosures made to NCA.

# CHAPTER 2: OFFENCES

## Introduction

There are a number of pieces of legislation that make up the UK’s Anti money laundering/counter terrorist financing legal framework. A brief summary of the main pieces of legislation is provided below. All employees of {NAME\_OF\_FIRM\_SHORT} should be aware that it is not only the firm that is subject to the legislation but also the employees within the firm. Failure to comply with certain aspects of the legislation can result in an individual being subject to prosecution with the threat of a custodial sentence or fine.

## Proceeds of Crime Act 2002

The Proceeds of Crime Act 2002 (“POCA”) is the main piece of legislation dealing with individual criminal liability in relation to money laundering. Offences under POCA occur in relation to “criminal conduct” and/or “criminal property”, which are defined below.

### Criminal Conduct

Criminal conduct is a conduct which constitutes an offence in any part of the United Kingdom (or would constitute an offence in any part of the United Kingdom if it occurred there).

### Criminal Property

Property is criminal property if it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly), and the alleged offender knows or suspects that it constitutes or represents such a benefit.

It is immaterial:

1. who carried out the conduct
2. who benefited from it
3. whether the conduct occurred before or after the passing of POCA 2002

A person benefits from conduct if he obtains property, advantage or benefit as a result of or in connection with the conduct or any other conduct. Where the property is land, this includes a servitude, right or interest in relation to that piece of land.

Property is all property wherever situated and includes:

1. money
2. all forms of property, real or personal, heritable or moveable
3. things in action and other intangible or incorporeal property

### Concealing, Making Arrangements and Acquiring

It is a criminal offence under sections 327-329 POCA for any person, subject to certain exceptions, to conceal, make arrangements, acquire, use or possess criminal property including funds. This offence covers being part of an arrangement to facilitate the acquisition, retention, use or control of criminal assets by another person.

This offence is punishable by a maximum penalty of 14 years’ imprisonment and an unlimited fine.

### Concealing and Related

A person commits an offence if he:

1. conceals criminal property
2. disguises criminal property
3. converts criminal property
4. transfers criminal property
5. removes criminal property from England, Wales, Scotland or Northern Ireland

This offence is punishable by a maximum penalty of 14 years’ imprisonment and an unlimited fine.

### Arrangements

A person commits an offence if he 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.

This offence is punishable by a maximum penalty of 14 years’ imprisonment and an unlimited fine.

### Acquisition, Use and Possession

A person commits this offence if he:

1. acquires criminal property
2. uses criminal property
3. has possession of criminal property

This offence covers any conduct wherever it takes place, if it would constitute a criminal offence if committed in the UK. This excludes minor offences committed overseas where the conduct is lawful in the jurisdiction where the offence in question is committed (for example, bull fighting in Spain). This offence however includes, but is not restricted to, drug trafficking, terrorist activity, corruption, theft, fraud, tax evasion, robbery, forgery, product piracy, illegal deposit taking, blackmail and extortion.

It is a **defence** to show that a person reported their suspicion to the MLRO (in the case of the MLRO, to a law enforcement agency).

This offence is punishable by a maximum penalty of 14 years’ imprisonment and an unlimited fine.

### Tipping Off

It is a criminal offence under section 333 POCA to take action likely to prejudice an investigation by informing (tipping off) the subject of a suspicion report, or anyone else, that a disclosure has been made to either NCA or the MLRO or that the police or customs authorities are carrying out or intending to carry out a money laundering investigation.

It is a **defence** to show that a person had either lawful authority or reasonable excuse to make the disclosure. It is also a defence that a person neither knew nor suspected that the disclosure would prejudice an investigation.

Tipping off is punishable by a maximum penalty of 5 years’ imprisonment and an unlimited fine.

### Failure to Disclose

It is a criminal offence under sections 330 and 331 POCA for persons working in the regulated sector not to disclose if they have reasonable grounds to know or suspect, in the course of their employment, that another person is engaged in money laundering, as soon as reasonably practicable after the information comes to their attention. This offence also covers a failure of the MLRO to report a suspicion to NCA without a reasonable excuse.

Reporting to the MLRO in accordance with {NAME\_OF\_FIRM\_SHORT}’s procedures will satisfy the obligation to report.

Legislation protects those reporting suspicions of money laundering from claims in respect of any alleged breach of client confidentiality.

Failure to disclose is punishable by a maximum of 5 years’ imprisonment and an unlimited fine.

**NOTE:** There is a separate offence of a failure to report reasonable knowledge or suspicion of terrorist fund raising, use and possession of terrorist funds and arrangements facilitating the retention and control of terrorist property.

### Destruction of Documents

It is an offence under section 341 POCA to destroy or dispose of documents that may be relevant to a money laundering investigation.

## Money Laundering Regulations 2017

The Money Laundering Regulations 2017 (“the Regulations”) implement the 3rd EU Money Laundering Directive. Approved amendments have also been made in September 2011 and December 2013. The 4th Money Laundering Directive commences from 26th June 2017. The purpose of the Regulations is to specify arrangements which must take place within banks to forestall and prevent operations relating to money laundering and terrorist financing.

{NAME\_OF\_FIRM\_SHORT} ’s business activities are within the scope of the Regulations and must therefore have in place appropriate policies and procedures covering:

* Customer due diligence
* Reporting
* Record keeping
* Internal control
* Risk assessment and management
* Compliance management; and
* Communication

The FCA may institute proceedings for offences under the regulations relating to money laundering. Whether a breach of the regulations has occurred is not dependent on whether money laundering has taken place. {NAME\_OF\_FIRM\_SHORT} is aware that they be sanctioned for not having adequate procedures in place.

**Failure to comply with the Regulations constitutes an offence punishable by a maximum of 2 years imprisonment, or a fine, or both.**

## Terrorism Act 2000 & the Anti-terrorism, Crime and Security Act 2001

The Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001) establishes offences related to involvement in facilitating, raising, possessing or using funds for terrorism purposes, failing to report, tipping off or prejudicing an investigation. The Act:

* Makes it a criminal offence for any person not to report the existence of terrorist property where there are reasonable grounds for knowing or suspecting the existence of terrorist property
* Makes it a criminal offence for anyone to take any action likely to prejudice an investigation by informing (i.e. tipping off) the person who is the subject of a suspicion report, or anybody else, that a disclosure has been made to a MLRO or to NCA, or that the police or customs authorities are carrying out or intending to carry out a terrorist financing investigation
* Grants a power to the law enforcement agencies to make an account monitoring order, similar in scope to that introduced under POCA

Failure to report is punishable by a maximum penalty of 5 years’ imprisonment and a fine. The offence of actual money laundering is punishable by 14 years’ imprisonment and a fine.

The Anti-Terrorism, Crime and Security Act 2001 gives the authorities power to direct firms in the regulated sector to provide the authorities with specified information on clients and their terrorism-related activities.

## US Legal Obligations

The US criminal money laundering laws, in particular the USA Patriot Act 2001, have extra-territorial effect. Where {NAME\_OF\_FIRM\_SHORT} has any established activities in, or linked to the USA, whether through a branch, subsidiary, associated company or correspondent banking relationship there is a risk that US regulations and sanctions may apply. This includes dealing with clients that are US citizens.

## Office of Foreign Assets Control (OFAC)

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

​The Treasury Department has a long history of dealing with sanctions. Dating back prior to the War of 1812, Secretary of the Treasury Gallatin administered sanctions imposed against Great Britain for the harassment of American sailors. During the Civil War, Congress approved a law which prohibited transactions with the Confederacy, called for the forfeiture of goods involved in such transactions, and provided a licensing regime under rules and regulations administered by Treasury.

OFAC is the successor to the Office of Foreign Funds Control (the ``FFC''), which was established at the advent of World War II following the German invasion of Norway in 1940. The FFC program was administered by the Secretary of the Treasury throughout the war. The FFC's initial purpose was to prevent Nazi use of the occupied countries' holdings of foreign exchange and securities and to prevent forced repatriation of funds belonging to nationals of those countries. These controls were later extended to protect assets of other invaded countries. After the United States formally entered World War II, the FFC played a leading role in economic warfare against the Axis powers by blocking enemy assets and prohibiting foreign trade and financial transactions.

OFAC itself was formally created in December 1950, following the entry of China into the Korean War, when President Truman declared a national emergency and blocked all Chinese and North Korean assets subject to U.S. jurisdiction.

The OFAC Main Page can be found at <http://www.treasury.gov/about/organizational-structure/offices/pages/office-of-foreign-assets-control.aspx>

## OFAC Sanctions Lists

**​Specially Designated Nationals List** Page found at <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>.

**​Consolidated Sanctions List**​ found at <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx>.

**Search OFAC's Sanctions** Lists found at <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fuzzy_logic.aspx>.

**Additional OFAC Sanctions Lists**​ found at <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/Other-OFAC-Sanctions-Lists.aspx>.

**Sanction Programs**

Currently there are a number of sanction programs in operation internationally. {NAME\_OF\_FIRM\_SHORT} is required by law to ensure full compliance and ensure that any links are identified, directly or indirectly. Such links may include:

- Jurisdiction of where an entity is registered;

- Jurisdiction of where an entity is operating;

- Beneficial ownership and control;

- Any other significant link to an individual or entity, which has been identified as a Specially

Designated National (“SDN”).

In consideration of this, where one of the above criteria is indicated for a prospective client, the AML Compliance Officer should escalate to the MLRO for review, who may seek legal advice from {NAME\_OF\_FIRM\_SHORT}.s General Counsel if required.

The full list of current programs in operation in the UK can be found at the following links:

* Al-Qaida & Taliban
* Belarus
* Burma/Myanmar
* Democratic Republ
* ic of Congo
* Eritrea
* Federal Republic of Yugoslavia & Serbia
* Iran
* Iraq
* Ivory Coast
* Lebanon and Syria
* Liberia
* Libya (lifted – but still requires consideration)
* North Korea (Democratic People’s Republic of Korea)
* Republic of Guinea
* Somalia
* Sudan
* Terrorism and terrorist financing
* Tunisia
* Zimbabwe

<https://www.gov.uk/current-arms-embargoes-and-other-restrictions>

All new account openings must ensure that all prospective client names are subject to KYC screening which will check applicable international sanction lists. In accordance with the risk matrix, it may be necessary to also check all directors and shareholders, ensuring that they are added to the ongoing screening database where deemed necessary.

As a matter of good practice, for high risk clients the MLRO may deem it necessary to independently review the HM Sanctions List and run an OFAC search using the sources listed below:

<https://ofac.finra.org/#/>

If in doubt about the nature of any of the information listed in the sanctions section, speak with the MLRO.

# CHAPTER 3: INTERNAL COMMUNICATIONS

## Money Laundering Reporting Officer

{NOFMLRO} is {NAME\_OF\_FIRM\_SHORT}’s Money Laundering Reporting Officer (“MLRO”). The MLRO has overall responsibility for the establishment and maintenance of effective anti-money laundering systems and controls.

The MLRO is a required Controlled Function the performance of which by a person requires FCA approval of that person. The FCA expects the MLRO to be based in the UK and to be of sufficient seniority within {NAME\_OF\_FIRM\_SHORT} to be able to act on his own authority. The MLRO must have access to all Know Your Business information. The MLRO’s responsibilities include the following:

* Monitoring of the effectiveness of {NAME\_OF\_FIRM\_SHORT}’s anti-money laundering controls
* Overseeing the firm’s compliance with the FCA’s rules on anti-money laundering systems and controls
* Having overall responsibility for the day-to-day operation of such policies, even where these have been delegated
* Ensuring that client account opening standards are compliant with {NAME\_OF\_FIRM\_SHORT}’s policy and the JMLSG
* Receiving and reviewing internal disclosures and submitting external reports to NCA
* Responding promptly to any reasonable request for information made by the FCA or law enforcement
* Liaising with the FCA, NCA and other external agencies
* Ensuring that anti-money laundering training is provided, its standards and scope are appropriate and that records are kept
* Reporting to the senior management on at least an annual basis (via a MLRO Report) and keeping the management updated on money laundering issues
* Obtaining and using national and international findings, for example the findings of the Financial Action Task Force (FATF), International Monetary Fund and World Bank
* Appointing of a Deputy MLRO to cover the MLRO’s periods of absence (NB: If the MLRO is temporarily unavailable for 12 weeks or more in any consecutive 12-months period, FCA pre-approval is required )
* Ensuring that client and transaction monitoring is being undertaken
* Assessing the risks of {NAME\_OF\_FIRM\_SHORT}’s client base and business activities in relation to money laundering on an on-going basis
* Ensuring the firm’s policies and procedures are being communicated effectively to all relevant employees.

While the MLRO may delegate their duties to another appropriate person, such delegation needs to be documented. In such cases the FCA will expect the MLRO to take ultimate managerial responsibility.

## Contact with Third Parties

{NAME\_OF\_FIRM\_SHORT} ’s personnel must not discuss any issues relating to the firm’s anti-money laundering policies and procedures with any third parties without prior consent of the MLRO. All requests from the FCA, NCA, Police, HM Revenue & Customs or other investigating and enforcement agencies must be referred to the MLRO without delay.

## Orders

The following orders may be served on {NAME\_OF\_FIRM\_SHORT} as part of an on-going investigation. Should you receive any such order, please give it to the MLRO without delay:

* a production order
* a disclosure order
* a customer information order
* an account monitoring order
* a search and seizure warrant
* an order for financial information under the Terrorism Act 2000

# CHAPTER 4: THE RISK BASED APPROACH

## Introduction

{NAME\_OF\_FIRM\_SHORT} is required to operate a risk based policy in order to identify, manage and mitigate the risks associated with the firm being used for money laundering or terrorist financing. This approach will identify the most cost effective and proportionate way to manage and mitigate the risks posed to the firm. It is accepted that a risk based regime cannot be a zero failure regime but that it should strike a balance between cost and the realistic threat of being used for money laundering or terrorist financing. The aim is to focus the efforts where they are most needed and will have most impact.

A risk based approach requires {NAME\_OF\_FIRM\_SHORT} to undertake the following steps:

* Assess the risks applicable to the firm. In the case of {NAME\_OF\_FIRM\_SHORT} these risks will predominately relate to our customers and the products and or services we provide to them.
* Design and implement controls to manage and mitigate these risks
* Monitor and improve the effective operation of the firm’s controls
* Record what has been done and why.

## Assessing the risk to {NAME\_OF\_FIRM\_SHORT}

{NAME\_OF\_FIRM\_SHORT} adopts a risk-based approach to business that enables it to utilise its resources in the most efficient and cost-effective manner. While we will, as far as reasonably practicable, ensure consistent application of our risk-based approach, we recognise that this approach cannot anticipate every eventuality. Therefore in any given case the Compliance Officer or MLRO may exercise their judgment in deciding whether or not to deviate from the written policies. This judgment will be clearly reasoned and documented.

**Geographical location of the client and their business**

When and if {NAME\_OF\_FIRM\_SHORT} deals with clients located in countries without adequate anti-money laundering standards it will either obtain additional Customer Due Diligence information or perform more intensive monitoring of the client’s account. Countries presenting ahigh geographical risk are those where:

* Cash is the normal medium of exchange
* There is a politically unstable regime with high levels of public or private sector corruption
* That are known to be drug producing or drug transit countries
* Have been classified as countries with inadequacies in their anti-money laundering strategies

A useful source of information on geographical risk is Transparency International www.transparency.org

The Transparency International Corruption Perception Index is attached to the Handbook as Appendix 8. The up to date index can be found at <http://www.transparency.org/>. Downloading the information package provides a host of data and it is sub-divided into continents.

## Client Risk Assessment

{NAME\_OF\_FIRM\_SHORT}’s client base is divided into three risk categories: Low, Medium and High. The Compliance Officer or MLRO determines to which category a client belongs. They will record the basis of assessment for each client. Given the nature of business undertaken by {NAME\_OF\_FIRM\_SHORT} it is expected that the majority of our clients will be assessed as either Medium risk or High Risk.

The following should be used as guidance when applying a risk-based approach to the assessment of money laundering risk posed by each client. Consideration of the overall information held may alter the risk profile of the client.

### Low Risk

* Regulated financial institutions based in the UK; those located in EU, FATF or comparable jurisdictions.

A list of comparable jurisdictions can be found at Appendix 5.

A list of FATF member countries can be found at Appendix 5.

* Companies or their subsidiaries (50% or more) whose shares are traded on EU regulated market or equivalent exchange,

A list of such exchanges can be found at Appendix 5 to this Handbook.

* a third country identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism (within the meaning of section 1 of the Terrorism Act 2000(94)), money laundering, and the production and supply of illicit drugs;
* a third country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or non-governmental organisations—
* has requirements to counter money laundering and terrorist financing that are consistent with the revised Recommendations published by the Financial Action Task Force in February 2012 and updated in October 2016; and
* effectively implements those Recommendations.
* Reputable, well-known organisations, with long histories in their industries or large market capitalisation and with substantial public information about them and their principals and/or controllers.
* Clients represented by those whose appointment is subject to court approval or ratifications (e.g. executors)

### High Risk

* Relationships where a Politically Exposed Person (“PEP”) or their connected person, have been identified as having a significant involvement.

This definition of **PEP** would include heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned enterprises and important political party officials. Please consult the MLRO if you think that you may be dealing with PEP or their connected person. (See Chapter 6 of this handbook)

* Complex business ownership structures, such as offshore special purpose vehicles, that make it easier to conceal underlying beneficial owners, especially where there is no legitimate commercial rationale.
* Accounts that involve regular payments to or from unrelated third parties.
* Names that have been previously linked with financial crime.
* Clients based in or conducting business in or through high-risk jurisdictions with known level of corruption and organised crime, or drug production and distribution.
* Clients engaged in higher risk business activities, for example where large amounts of cash are involved.
* Companies issuing bearer shares, especially if incorporated in higher risk jurisdictions.
* Clients that have been subject to a Suspicious Transaction Report.
* Clients that have not been physically present for identification purposes. This does not apply to clients to whom SDD applies.

### Medium Risk

All other clients that do not fall within either a low-risk category or a high-risk category including (but not restricted to):

* Subsidiaries of or entities associated with low-risk clients
* Private companies from the UK, EEA or comparable jurisdiction provided they are not undertaking high risk business.

## Additional Considerations

{NAME\_OF\_FIRM\_SHORT} will take the following additional considerations into account when determining the risk posed by a particular client. While these considerations will not determine the risk on their own, they will be considered alongside other factors in judging the overall money laundering risk posed by a particular client.

* Whether {NAME\_OF\_FIRM\_SHORT} is engaged in a one-off transaction or business relationship
* In relation to introduced business, the effectiveness of the due diligence carried out by the introducer
* The nature and length of any existing or previous relationship between either {NAME\_OF\_FIRM\_SHORT} or our employees and the client
* The way in which information is obtained (e.g. from a government department, regulated firm or other source)
* The nature and extent of any assurances given by other regulated firms that may be relied upon.
* Any associations the client may have with other entities or jurisdictions, such as headquarters, operating facilities, branches or subsidiaries and the individuals who may influence its operations.
* Other relevant considerations; such as whether the client has a regulated investment manager or adviser, a prime broker (who have performed due diligence on the client) and other considerations that the Compliance Officer or MLRO may reasonably consider relevant to the client’s risk assessment.
* The type of products or services that {NAME\_OF\_FIRM\_SHORT} is providing to the client.

## MLRO’s On-going Risk Assessment

Risk management is a continuous process. The MLRO is responsible for ensuring the firm’s risk assessment is up to date and appropriate. This is done by means of an on-going risk assessment.

On an on-going basis the MLRO will review {NAME\_OF\_FIRM\_SHORT}’s business activities, including:

* Appropriate procedures to identify changes in client characteristics, which come to light in the normal course of business
* Ways in which different products and services may be used for money laundering or terrorist financing, and how these ways may change
* Adequacy of staff training and awareness
* Monitoring compliance arrangements (such as internal audit/quality assurance, processes or external review)
* The balance between technology-based and people-based systems
* Capturing appropriate management information
* Upward reporting and accountability
* Effectiveness of the liaison with regulatory and law enforcement agencies

The MLRO will identify any changes to {NAME\_OF\_FIRM\_SHORT}’s services that may expose the firm to a higher risk of money laundering. This may also highlight the need for a formal assessment of risks posed by either of our client categories or individual clients. The results of this on-going assessment will be detailed in the annual MLRO’s Report to senior management.

# CHAPTER 5: CUSTOMER DUE DILIGENCE PROCEDURE

## Introduction

The new Money Laundering Regulations 2017 set out the firm’s obligations to conduct Client Due Diligence (“CDD”) in a more detailed form than under the previous regulations. The regulations now specify the CDD measures that are required to be carried out, the timing, as well as actions required if CDD measures are not carried out. The concept of Simplified Due Diligence (SDD) and Enhanced Due Diligence (EDD) are also introduced by the new regulations. The purpose of this chapter is to provide guidance on the following:

* The meaning of CDD measures
* Timing of, and non-compliance with CDD measures
* Application of CDD measures
* Simplified Due Diligence
* Enhanced Due Diligence

For lists of the documentation to be obtained and verified in respect of specific business types please refer to Chapter 6 of this handbook.

## What is CDD?

The CDD measures that must be carried out involve:

1. Identifying the customer and verifying the identity
2. Identifying the beneficial owner, where relevant, and verifying their identity
3. Obtaining information on the purpose and intended nature of the relationship
4. Conducting on-going monitoring of the relationship
5. In the case of legal entities the firm must understand the ownership and control structure.

These measures are designed to make it harder for the financial services industry to be used to launder money or fund terrorism.

We will apply CDD to all customers on a risk-sensitive basis, and this should entail considering at least the elements listed below and being able to show that the measures taken are appropriate:

• the purpose of the account or relationship;

• the level of assets to be deposited and size of transactions;

• the regularity or duration of the relationship; and

• including due diligence on beneficiaries of insurance or investment policies at the appropriate time.

## Timing of, and non-compliance with, CDD measures

{NAME\_OF\_FIRM\_SHORT} will ensure that it has completed appropriate client due diligence prior to entering into a legally binding agreement with the client to undertake regulated business. The Compliance Officer/MLRO may, at his discretion, allow an account to be opened before all the documentation has been obtained if it is necessary in order not to interrupt the normal conduct of business and there is little risk of money laundering. In these cases the decision must be fully documented and all outstanding documentation obtained as soon as possible. In these instances the firm should not make any payments from that account either to the client or to a third party until such times as the documentation has been obtained and verified.

If {NAME\_OF\_FIRM\_SHORT} is unable to comply with the required CDD measures in relation to a customer, then the firm must not undertake any transactions for that client and should terminate any existing relationship. At this point it will be necessary to consider making a Suspicious Transaction Report to the MLRO.

If the client does not possess the right documents then the firm should consider whether there are any other ways of being reasonably satisfied as to the client’s identity.

Where an account is to be terminated due to a lack of CDD the MLRO should be consulted as to the appropriate way to return the funds.

## Who is the Customer?

The term customer is not defined by the ML regulations but, in general, will be the party with whom the business relationship would be established. If in doubt as to who should be identified as the customer please seek guidance from the Compliance Officer or MLRO.

## Who is the beneficial Owner?

The ML Regulations require that anyone owning or controlling 25% or more of a legal entity is identified and that their identity be verified in line with the firm’s risk based approach.

## Existing Customers

If a client has already been identified by {NAME\_OF\_FIRM\_SHORT}, no additional information needs to be obtained in respect of such a client unless the information already available is either out of date; or if the client’s risk profile has changed. This may happen if the firm supplies a different product or service to the client or if {NAME\_OF\_FIRM\_SHORT} becomes aware of any information that results in a change to the client’s risk profile.

## Simplified Due Diligence

Simplified Due Diligence can be applied to certain low risk entities. Whilst this means there is no requirement to perform checks on the client’s identity or beneficial ownership structure it is necessary to prove that they fall within the SDD exemption. SDD can be applied to:

* Financial institutions in the UK, EU or comparable jurisdictions that are subject to the ML Regulations or equivalent
* Companies listed on a regulated market
* UK public authorities
* Legal and accountancy firms in the UK that are members of a recognised professional body (e.g. The law Society or the Institute of Chartered Accountants in England and Wales)
* Community institutions (e.g. European Investment Bank, Environment Agency, Europol)

Further detail on the application of SDD to these entities can be found in Chapter 6.

## Enhanced Due Diligence

Under the risk based approach adopted by {NAME\_OF\_FIRM\_SHORT} EDD will need to be conducted on any clients falling into the high-risk category. In addition to these clients the regulations state three specific types of relationship where EDD must be applied. These are:

* Where the client is not physically present
* In respect of correspondent banking relationships
* Any relationship or transaction involving a Politically Exposed Person (“PEP”)

Specific guidance on the application of enhanced due diligence is contained in Chapter 6.

## Account Opening Process

{NAME\_OF\_FIRM\_SHORT} will use a standard New Account Form to open new client accounts attached to this Handbook as Appendix 3.

## Exception to Full Identification

While we will use our standard account opening procedure to verify the identity our clients whenever possible; it may be the case that a client cannot provide standard information, or there are other factors that may influence the client’s risk-profile. {NAME\_OF\_FIRM\_SHORT}’s procedure cannot accommodate every eventuality and in some cases the Compliance Officer/MLRO will need to exercise their judgment. This may justify a deviation from the firm’s standard client opening procedure. All such exceptions must be agreed and documented by the Compliance Officer or MLRO in accordance with {NAME\_OF\_FIRM\_SHORT}’s risk-based approach.

## Capacity of the Client

### I. Client Acting as an Agent

#### Regulated Financial Sector Firms

When identifying a client that acts on behalf of underlying customers AND is either of the following:

1. An FCA regulated financial sector firm; or
2. A non-UK firm located in a comparable jurisdiction AND regulated by an overseas regulator

{NAME\_OF\_FIRM\_SHORT} will not need to identify the underlying customers, even if their identity is disclosed to us, unless we take instruction directly from the underlying customers.

In all other cases {NAME\_OF\_FIRM\_SHORT} will obtain identification and verification evidence in respect of both an intermediary and an underlying customer in accordance with our risk-based approach.

#### Firms Located in Non-Comparable Jurisdictions

Unless we are satisfied that the agent firm operates client identification procedures equivalent to the UK standards, the underlying customers must be identified or business declined.

#### Unregulated Agents Based in Comparable Jurisdictions

Unless {NAME\_OF\_FIRM\_SHORT} is satisfied that the agent firm operates client identification procedures equivalent to the UK standards, the underlying customers must be identified or business declined.

### II. {NAME\_OF\_FIRM\_SHORT} Acting Solely as an Introducer

{NAME\_OF\_FIRM\_SHORT} may act solely as an introducer between the client and the firm providing a product or service (“Provider Firm”). {NAME\_OF\_FIRM\_SHORT} will play no part in the actual transaction and have no other relationship with either of the parties.

In such cases the identification and verification obligations will lie with the Provider Firm, and not with {NAME\_OF\_FIRM\_SHORT}, provided that:

1. {NAME\_OF\_FIRM\_SHORT} does not give advice to the client; and
2. {NAME\_OF\_FIRM\_SHORT} does not play any part in the negotiation or execution of the transaction;

unless {NAME\_OF\_FIRM\_SHORT} is acting as an agent of the Provider Firm.

## Standard of Verification Evidence

### Client Risk

The level of documentation required for each client will vary depending on the risk category of a particular client.

### Financial Services Targets

It is a criminal offence to make funds or financial services available to sanctioned entities and people (targets) on the list maintained by the HM Treasury. This would include dealing directly with these targets, and dealing with these targets through intermediaries (such as lawyers or accountants).

Please contact the MLRO for the [Bank of England Consolidated List of Financial Sanctions Targets](https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets).

### Origin of Documents

Generally, when identifying a client, a document issued by a government department or agency, or by a court will provide a high level of confidence. {NAME\_OF\_FIRM\_SHORT} will normally accept non-government issued documentary evidence verifying identity only if it originates from a public sector body or a regulated financial services firm in a comparable jurisdiction, or is supplemented by knowledge that {NAME\_OF\_FIRM\_SHORT} has of the person or entity, which it has documented (please refer to Section B2 box 7 the NAO Form in Appendix 3).

### Home Visit Evidencing Address

If {NAME\_OF\_FIRM\_SHORT}’s employee has visited the client at their business (or home, for individuals) address, a record of this visit may constitute evidence corroborating that the client is located at this address (i.e. as a second document).

### Documents in a Foreign Language

If documents are in a foreign language, {NAME\_OF\_FIRM\_SHORT} will take appropriate steps to be reasonably satisfied that the documents do in fact provide evidence of the client’s identity. This is likely to involve translation of either all or part of a document.

### Documentary and Electronic Evidence

{NAME\_OF\_FIRM\_SHORT} may rely on either documentary, electronic or a combination of documentary and electronic identification evidence. If we choose to rely on electronic evidence only, we must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. We cannot rely exclusively on electronic systems that access data from a single source only (e.g. a single check against the Electoral Roll). For further information on the use of electronic evidence please consult the Compliance Officer or MLRO.

### Certification of Documents

Where possible, we will seek to obtain certified copies of identification documents. In these cases each document needs to contain a statement that the document is a certified copy of the original and must be dated and signed by one of those, listed in the non-exhaustive list detailed below:

* Solicitor or notary public
* Banker
* Auditor or Accountant
* Consulate or government official
* {NAME\_OF\_FIRM\_SHORT} ’s employee who has seen the original.

In addition, a person who certifies a document should provide their contact details.

{NAME\_OF\_FIRM\_SHORT} will generally not accept documents certified by an officer of the client.

### Clients’ Websites

{NAME\_OF\_FIRM\_SHORT} understands that although the information on the websites of its clients or potential clients may be helpful, it is not independently verified. While {NAME\_OF\_FIRM\_SHORT} may use such information as corroborative evidence, it will not exclusively rely on it; an exception can be made by the Compliance Officer/MLRO for low risk clients.

### Public Information

Listed and some unlisted public companies are subject to a high level of disclosure in relation to ownership and business activities; and may have public filing obligations. Private companies and some partnerships, although not subject to such a level of disclosure, often have public filing obligations. Whenever possible and appropriate, {NAME\_OF\_FIRM\_SHORT} will seek to use reliable public information in its identification process.

### Signatories

On some occasions, and where appropriate, {NAME\_OF\_FIRM\_SHORT} may be provided with a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give {NAME\_OF\_FIRM\_SHORT} such instructions. {NAME\_OF\_FIRM\_SHORT} will use this information in determining whom to identify, using its risk-based approach.

### Non Face To Face Clients

Given {NAME\_OF\_FIRM\_SHORT}’s business model, it is unlikely we would not meet our clients face to face.

Given our business and the type of service we provide, it is unlikely that clients accepted in such a manner will be deliberately avoiding face-to-face contact. Therefore non face-to-face business will not in itself magnify a money laundering risk posed by a particular client. However non face-to-face identification carries an inherent risk of impersonation fraud. To address this risk {NAME\_OF\_FIRM\_SHORT} will perform at least one additional verification check for non-face to face clients, such as:

* Verifying **additional aspects** of the client’s identity (or the same or different aspect of identify by electronic means)
* Sending Terms of Business or other applicable documentation to a verified address (to be signed and returned by the client)
* Requiring copy documents to be certified by an appropriate person

### Controller of Funds

If it appears that another person may have control over the funds which form or otherwise relate to the relationship with our client, we will seek to identify the controller as well as the client, if and when justified by risk.

* SOW – Statement of Wealth – this can be a certified HNW certificate.
* SOF – Source of Funds – through ongoing transaction monitoring iaw MLR 2017 Regulation 35.
* SOW & SOF – definitely required for PEP and High-Risk Customers iaw MLR 2017 Regulation 35.

Documents evidencing each item declared on SOW is a requirement under Money Laundering Regulations 2017 which incorporate the EU 4th Directive on Money Laundering.

Each declaration on the SOW or assets owned by the customer must be evidenced by documentation and should be independently verified. A verifiable Chartered Accountant’s letter would be acceptable, ideally categorising the cash, property, shareholdings and

Should the bank decide to take a reduced risk approach on some PEP customers a SOW is required with evidence supporting the wealth taken from publicly available information, transaction records (statements) and searches.

UK/EU domestic PEPs should be initially treated as a PEP and when the KYC Analyst is satisfied that there is no other involvement or concern, they can be risk assessed and treated with a lower level of due diligence (Regulation 35 MLR 2017). These PEPs can, if the business relationship is not High Risk, be approved at departmental manager level.

### Source of funds

**Income from Employment**

An original or certified copy of a recent pay slip- last pay slip within 3 months

Written confirmation of salary signed by employer.

**Property Sale**

* Original or certified copy of contract of sale
* Written confirmation of sale signed by advocate/solicitor

**Sale of Investments**

* Original or certified copy of contract notes
* Written confirmation of sale/holding signed by accountant/broker

**Inheritance**

* Original or certified copy of will or grant of probate
* Written confirmation of inheritance signed by advocate/ trustee/ executor.

**Company Sale**

* Original or certified copy of contract of sale
* Written confirmation of sale signed by advocate/solicitor
* Internet research of Company Registry

**Divorce Settlement**

* Original or certified copy of Court Order
* Written confirmation of settlement signed by advocate / solicitor.

**Savings**

Statement from the savings institution – 3 months - and enquiry of the source of wealth

**Lottery / Gambling win**

* Evidence from the lottery company
* Cheque
* Winnings receipt

**Companies**

Accounts – latest/last annual

* Industry sector clients
* New venture/products clients
* Any other relevant areas you consider necessary

### Controllers and Beneficial Owners

We must ensure that controllers and Ultimate Beneficial Owners (UBO) of entities are identified and verified.

Appropriate identification, verification and due diligence must be completed. Where required we should take sufficient measures to reach a good understanding of the underlying structure and ownership by considering information such as:

* the legal form of the Entity (for example corporation, limited company, partnership, trust etc; and
* the controllers of the company (for example knowledge of who within the Entity is authorised to make major decisions, such as executive management or executors)

The standards for identification and verification set-out earlier in this Policy must be used to verify and identify controllers or UBO’s.

### Other Considerations

Passport copies should be in black and white, not colour (wherever possible).

Clients should be discouraged from sending original valuable documents by post.

Consideration should be given as to whether the documents relied upon may have been forged.

# CHAPTER 6: IDENTIFICATION EVIDENCE

## Introduction

The purpose of this section of the manual is to provide detailed guidelines to staff in respect of obtaining account opening documentation. The information below covers the types of legal entity that are likely to be clients of {NAME\_OF\_FIRM\_SHORT} . However, due to the diversity of legal structures in place it is not possible to cover all possible scenarios below. If a potential new client does not appear to fit into any of the categories detailed below you should seek guidance from the MLRO as to the most appropriate type of documentation to obtain.

There are five parts to Customer Due Diligence

1. Knowing who the applicant for business is (identification)
2. Is the client who they say they are (verification)
3. Ascertaining the nature and purpose of the relationship
4. Keeping information up to date
5. Ongoing monitoring to assess if in line with what is expected

This chapter covers the first three steps

## Clients entitled to Simplified Due Diligence (SDD)

### Regulated Financial Institutions

Where the new client is a regulated financial institution in the UK, EU, FATF or comparable jurisdiction there is no requirement to perform identity or verification checks. It is however a requirement that {NAME\_OF\_FIRM\_SHORT} has reasonable grounds for believing the customer is an institution covered by SDD.

Therefore when dealing with regulated firms {NAME\_OF\_FIRM\_SHORT} will obtain the following information:

* The evidence of the client’s regulated status; AND
* The evidence of the client’s address

The list of regulators provided in Appendix 5 will assist {NAME\_OF\_FIRM\_SHORT} in identifying such clients.

### UK Public Authorities and Community institutions

In respect of UK public authorities and community institutions {NAME\_OF\_FIRM\_SHORT} may apply SDD.

Therefore, when dealing with a UK public authority or community institution {NAME\_OF\_FIRM\_SHORT} will obtain the following information:

* The evidence of the client’s public status; AND
* The evidence of the client’s address

### Companies listed on an EU regulated market or equivalent exchange.

Companies listed on an EU regulated market or equivalent exchange are publicly owned and accountable.

For all such customers {NAME\_OF\_FIRM\_SHORT} will obtain the evidence of address as well as reliable evidence that the client is either of the following:

* A publicly quoted company (that is subject to public disclosure rules), or
* A 50% (or more) consolidated subsidiary of a publicly quoted company

Whilst the SDD standards are lower for the types of client mentioned above it does not negate the need to obtain and verify further information if the risk assessment of the new clients suggests this may be appropriate.

If a regulated market is located within the EEA there is no requirement to undertake checks on the market itself. {NAME\_OF\_FIRM\_SHORT} will however, record the steps it has taken to ascertain the status of the market. 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.

### Companies subject to the licensing and prudential regime of a statutory regulator in the EU

This would include companies that are subject to regulators such as OFWAT OFGEM or OFCOM or an EU equivalent e.g. power and telecommunications companies.

**Members of recognised professional bodies**

This will include legal and accountancy firms in the UK that are members of a recognised professional body (e.g. The law Society or the Institute of Chartered Accountants in England and Wales). {NAME\_OF\_FIRM\_SHORT} will obtain appropriate evidence that the firm is a member of the recognised professional body and this will be held on file.

## Clients Subject to Full Identification Requirements

**Unregulated Private Companies and Limited Partnerships**

### Introduction

{NAME\_OF\_FIRM\_SHORT} , when identifying a company or limited partnership will seek to understand its legal form, ownership structure and business. The amount of information that we will seek to obtain will depend on the money laundering risk posed by a particular company. Money Laundering Risk is discussed in Chapter 4.

Different information requirements in relation to different types of entity are detailed below. For all such clients {NAME\_OF\_FIRM\_SHORT} as a matter of course will seek to obtain the following Standard Information; that is information required for all clients. Additional information will need to be obtained in relation to Medium and High risk clients.

### Standard Information for Medium Risk Clients

{NAME\_OF\_FIRM\_SHORT} will obtain the following standard information in respect of each corporate client. The extent of verification of this information will depend on the risk posed by a particular client. When verifying the identity of a client in accordance with a risk based approach, we will take into account the below mentioned examples of documentation that can be used for such verification.

1. An official document containing the client’s **full name and registered number**

Examples:

* A copy of Certificate of Incorporation or Partnership Agreement (if any)
* Companies House (or equivalent registry) search

1. Evidence of client’s **registered office** in the country of its incorporation

Examples:

* A confirmation of the address by a reputable professional person
* Companies House (or equivalent registry) search

1. Evidence of client’s **business address**

Examples:

* A copy of a utility bill;
* A government issued document
* A record of visit to the client’s place of business

1. **Names of all directors**
2. Names of all direct and indirect **beneficial owners** owning 25% or more of the entity

Where no beneficial owner has an interest of 25% or more, the Compliance Officer will determine whose identity should be verified, taking a risk-based approach.

1. Copy of latest **audited accounts** where available.
2. A group / shareholding chart (where relevant)

Wherever possible this information must be obtained from an independent source such as Companies House or from a reputable business information provider. Further detail of the standard of evidence is given in Chapter 5.

**The identity of beneficial owners owning 25% or more of the company and the identity of at least one director must be verified in line with the requirements for private individuals.**

### For Limited Partnerships which are Medium Risk Clients

Limited Partnerships are treated in the same way as a private company the only difference being a list of partners will be obtained in place of the lists or directors and beneficial owners.

The identity of the partners or other beneficial owners with a beneficial interest of 25% or more of the partnership, including the General Partner/Managing Partner, must be verified in line with the requirements for private individuals.

If the General Partner/Managing Partner is a corporate entity, the identity of the ultimate beneficial owner of that corporate entity must be verified.

### High Risk Clients

In relation to High risk clients we will obtain at least the following information, additional to both the standard information for Medium risk clients (save for overlapping requirements), or both:

1. Identification information for two executive directors (if applicable), in accordance with identification requirements for individuals; AND
2. In respect of Politically Exposed Persons (“PEPS”) senior management approval will need to be obtained together with details of source of funds/wealth involved.

### Legal and accountancy firms

## Firms that are members of a recognised professional body (accountants and lawyers) will often be set up as limited companies or partnerships. As they will be classified as low risk from a money laundering perspective {NAME\_OF\_FIRM\_SHORT} has decided that there is no need to obtain the various documents that would apply to a private company or partnership that was not a member of a recognised professional body (Medium Risk Clients).Partnerships

{NAME\_OF\_FIRM\_SHORT} will treat partnerships and other unincorporated businesses in accordance with the requirements and guidelines set out above for private companies (as noted in page 22 this will not apply to partnerships that are members of a recognised professional body). The standard information for all such businesses will consist of:

1. Evidence of trading address
2. Nature of business activities
3. List of all partners
4. Copy of partnership deed
5. A copy of the latest (audited, where available) financial statements.

The identity of the partners or other beneficial owners with a beneficial interest of 25% or more of the partnership must be verified in line with the requirements for private individuals.

If any of the partners is a corporate entity, the identity of the ultimate beneficial owner of that corporate entity must be verified in accordance with the requirements for individuals.

## Non UK Governments and Public Authorities

When accepting a new client that is a government body or public authority in a country other than the UK the approach to identification and verification has to be tailored. Guidance below should be sufficient to identify and verify most organisations but in the case of any doubt please seek advice from the MLRO.

The following information should be obtained:

* Full name of entity
* Nature and status of entity
* Address of entity
* Name of home state authority
* Names of directors (or equivalent)

The firm will verify the name, address and where possible the home state authority.

For higher risk organisations the firm will undertake verification of identity on two directors.

## Trusts, Foundations and Similar Entities

It is unlikely that our client base will include trusts. However we do not rule out the possibility that we may be dealing with a trust. {NAME\_OF\_FIRM\_SHORT} will treat trusts in accordance with its risk-based approach. In relation to trusts we will have regard to the following considerations, as well as to the general considerations outlined above in implementing our risk-based approach:

* Transparency of the trust’s activities
* Complexity of the trust’s structure (e.g. the presence of numerous layers of ownership)
* Location of the trust (e.g. in a “tax-haven” previously associated with money laundering)

In many cases a trust will not be a separate legal entity but should still be regarded as the customer. The trustees of a trust will be considered the controllers. The purpose and objects of most trusts are set out in a trust deed. Please consult the Compliance Officer or MLRO if you are unsure as to who your client is.

Most trusts accepted as clients of {NAME\_OF\_FIRM\_SHORT} will fall into the medium risk category. If the trustees of a trust are all regulated entities or publicly listed companies it may be possible to consider them low risk if there is nothing to suggest they should be treated otherwise. For each trust we will seek to obtain the following information:

* Full name of the trust
* Nature and purpose of the trust (e.g., discretionary, testamentary, bare)
* Country of establishment of the trust
* Names of all trustees
* Names of any beneficial owners (see below concerning verification)
* Name and address of any protector or controller

If the client is to be low risk then it will be necessary to demonstrate that all trustees (i.e. controllers) are either regulated institutions or listed companies.

### Medium Risk Trusts

Trusts set up under testamentary arrangements and small, local trusts funded by small, individual donations from local communities, serving local needs, will be classified as Medium risk.

In addition to verifying information in accordance with procedures for Low risk clients, we will obtain the following information:

* **Either** a register search in the country of establishment;
* **Or** a summary of the instrument establishing the trust.

### High Risk Trusts

Offshore trusts and trusts with complex structures will be classified as High risk. In respect of High risk trusts {NAME\_OF\_FIRM\_SHORT} will seek to obtain and, where appropriate, verify some or all the following additional information in addition to the information required for Low and Medium risk clients:

* Names of the donor, settlor or grantor of the funds (where there are large numbers of small donors, donors of 10% or more only)
* Domicile of business/activity
* Nature of business or activities of the trust
* Operating address of the trust
* Names and/or classes of the trust’s beneficiaries
* Deed of Trust;
* Memorandum and Articles of Association;
* Certificate of Incorporation;
* Registered address and business address;
* List of Trustees;
* Full ID proof of Trustees, passports, addresses, verification, Thomson Reuters;
* Signatures;
* Power of Attorney;
* In case of a charitable trust – the Charity Commission Register number;
* Name of settlor or dummy settlor/protector/beneficiary (note - these are often the same person);
* Full ID proof of Trustees, passports, addresses, verification, Thomson Reuters;
* Statement of source of wealth;
* Witnessed Mandate to open account

### UK & Non UK Charities

### The following information must be obtained for all UK and non-UK registered charities - prior to opening the account:

• Full legal name

• Company registered number and charity registration number

• Registered office in the country of incorporation

• Business address

• Nature of the company’s business

• Completion of the Bank’s account opening form

• Latest accounts

• Mandate to open account

• Statement of source of wealth (funds-donations, size and regularity)

• Beneficial owners

• ID, passport, ID card, proof of address

• Statement of source/s of funds

### Beneficial owners

For all trusts the identity of the beneficial owners will need to be verified. These will be

* + The trustees or individuals having control over the trust
  + 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

Following its assessment of the money laundering risk presented by the trust, the firm may decide to verify the identities of additional trustees, and/or of the settlors.

### Private Individuals

In cases where {NAME\_OF\_FIRM\_SHORT} needs to identify a private individual, it will always seek to obtain the following information:

* Full name
* Residential address
* Date of birth

In verifying the individual’s identity we will obtain:

**EITHER:**

**A. A government-issued document which incorporates:**

* The client’s full name and photograph; **AND**
  + **Either** their residential address;
  + **Or** their date of birth

**OR:**

**B. A government-issued document (without a photograph) which incorporates the client’s  
 full name,**

**SUPPORTED BY:**

A second document, either government-issued, or issued by a judicial authority, a public sector body or authority, or another FCA regulated firm in the UK financial services sector, or in a comparable jurisdiction, which incorporates:

* The client’s full name; **AND**
* **Either** their residential address;
* **Or** their date of birth

Client identification performed electronically should mirror the above requirements.

Where business is conducted face-to-face, we will, whenever possible, seek to review the originals of any documents involved in the verification.

In the case of private individuals that have not been met by the firm an additional piece of acceptable documentation must be obtained.

Please refer to Appendix 4 for a non-exhaustive list of acceptable documents for individual identity verification.

**If the client has been deemed to be of higher risk then the following applies:**

##### Verifying the identity of higher risk individuals

Full name, date and place of birth must be verified using either:

a) a current passport (to include the photograph page and pages containing reference numbers, date country of issue, nationality and place of birth); or

b) a national identity card ((to include the photograph page and pages containing reference numbers, date country of issue, nationality and place of birth).

##### Verification the address of higher risk individuals

At least one of the following original documentary evidence confirming the individual’s current residential address is required for all relationships classified as medium or high risk.

(The documents are listed in order of preference - Not all documents are appropriate in some countries):

a) Current national identity card (if not used to verify identity)

b) Current photographic driving licence

c) Correspondence from a central or local government department or agency e.g. tax assessment or notice of tax code (issued during the previous 12 months)

d) Social security card (if current residential address is included)

e) Council tax demand letter or statement (issued during the previous 12 months);

f) Bank statement or credit card statement which shows your name and address (issued less than 3 months previously);

g) Mortgage statement (issued less than 3 months previously);

h) Utility bill (but not ones printed off the internet).

If an individual has lived at their current residential address for less than 12 months {NAME\_OF\_FIRM\_SHORT} will require a document which confirms the individual’s previous residential address. Please note – a C/O address or PO Box is not acceptable.

## Politically Exposed Persons (‘PEPS’)

It is necessary for enhanced due diligence (“EDD”) to be conducted where a client is a PEP or where one or more of the directors or beneficiary owners of a client are a PEP.

A PEP is defined as an individual who has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member or known close associate of such a person. The risks of Politically Exposed Persons (PEPs) are that they may handle proceeds of corruption and/or may offer, be offered or expect/demand bribes. A prominent public function could include, but is not limited to:

* Heads of state, heads of government, minister and deputy or assistant ministers
* Members of Parliament (MPs)
* Members of supreme courts or other high level judicial bodies
* Members of courts of auditors or of the boards of central banks
* Ambassadors, chargés d’affaires and high ranking officers in the armed forces
* Members of administrative, management or supervisory boards of state owned enterprises

There is no initial distinction between the locations of a PEP and the MLR 2017 identifies domestic (UK & EU) PEPs to be treated as a PEP.

Politically Exposed Persons, and family members or known close associates of PEPs, are individuals who by virtue of their position pose an inherently higher money laundering risk, particularly if they are based in a higher risk country or business. Money Laundering Regulations require us to monitor all PEP relationships due to the likelihood that they will pose a higher risk.

When taking on new customers and updating existing customer Identification and Due Diligence, we must screen customers against publicly available PEP lists in order to determine if they are politically exposed.

In respect of PEPs {NAME\_OF\_FIRM\_SHORT} must have

* senior management sign off on the ANOA
* evidence of the source of wealth and source of funds which are involved in the business relationship or transaction.

## FATCA & Global Intermediary Identification Number (GIIN)

**What is FATCA?**

The Foreign Account Tax Compliance Act (FATCA) is a 2010 United States federal law to enforce the requirement for United States persons including those living outside the U.S. to file yearly reports on their non-U.S. financial accounts to the Financial Crimes Enforcement Network (FinCEN).

GIIN is an abbreviation of Global Intermediary Identification Number. The FATCA Registration System approves foreign financial institutions (FFI), financial institution (FI) branches, direct reporting non-financial foreign entities (NFFE), sponsoring entities, sponsored entities, and sponsored subsidiary branches. Institutions and entities assigned a GIIN can use it to identify themselves to withholding agents and tax administrators for FATCA reporting purposes.

Is it only for US citizens? If an individual’s account holds any of the following seven criteria, we may need to request further information or documentation to determine if the customer is a US person under FATCA.

* US citizenship or US residence.
* US place of birth.
* US address including US PO boxes.
* US telephone number.
* Repeating payment instructions to pay amounts to a US address or an account maintained in the US.
* Current power of attorney or signatory authority granted to a person with a US address.
* In care of or hold mail address which is the sole address for the account holder.

## Other Considerations

* Passport copies should be in black and white, not colour (wherever possible).
* Clients should be discouraged from sending original valuable documents by post.
* Consideration should be given as to whether the documents relied upon may have been forged or altered in any way.

# CHAPTER 7: INTRODUCTIONS BY INTERMEDIARIES

## General Criteria

{NAME\_OF\_FIRM\_SHORT} may accept a confirmation from an intermediary that a client’s identity has been appropriately verified. We will take account of the following considerations when deciding whether it is reasonable for us to rely on an intermediary to have properly identified the client:

* The public disciplinary record of the intermediary, to the extent it is available.
* The nature of the client, the product or service sought and the sums involved.
* Any adverse experience of the intermediary’s general efficiency in business dealings.
* Any other knowledge, whether obtained at the outset of the relationship or subsequently that we have regarding the standing of the intermediary.

## Introducers

### Reliance on Third parties

### Where the business relies on a third party for compliance with this policy, or additional applicable AML requirements, the MLRO must ensure that such reliance is permissible under law and consistent with this policy, and reasonable under the circumstances.

### Regulation 39 of the MLR 2017 When a relevant person relies on the third party to apply customer due diligence measures under paragraph (1) it—

### must immediately obtain from the third party all the information needed to satisfy the requirements of regulation 28(2) to (6) and (10) in relation to the customer, customer’s beneficial owner, or any person acting on behalf of the customer;

### must enter into arrangements with the third party which—

### enable the relevant person to obtain from the third party immediately on request copies of any identification and verification data and any other relevant documentation on the identity of the customer, customer’s beneficial owner, or any person acting on behalf of the customer;

### require the third party to retain copies of the data and documents referred to in line with record keeping policy for the period required by {NAME\_OF\_FIRM\_SHORT}.

### Regulated Financial Sector Firms

Provided the introducer satisfies the general criteria above, {NAME\_OF\_FIRM\_SHORT} will normally be able to rely on an Introduction Certificate[[1]](#footnote-1) from an FCA regulated firm or regulated financial institution in a comparable jurisdiction.

### Professional Firms

{NAME\_OF\_FIRM\_SHORT} will not accept Introduction Certificates from lawyers, accountants and other professionals but may rely on the copies of verification documentation supplied by a professional firm to us, provided that these have been assessed by {NAME\_OF\_FIRM\_SHORT} as satisfactory.

### Firms in Non-Comparable Jurisdictions

If the introducing firm is located in a non-comparable jurisdiction, {NAME\_OF\_FIRM\_SHORT} will either:

1. Identify the introduced client itself; or
2. Rely on an Introduction Certificate if it is accompanied by copies of identification documents certified in accordance with UK standards.

## Group Introductions

Where a client is introduced by one part of a financial sector group to another, it is not necessary for their identity to be re-verified, provided that:

1. The client’s identity has been verified by the introducing part of the group in line with standards in the UK, EU or a comparable jurisdiction; and
2. A group introduction confirmation is obtained and held with the client’s records (except if {NAME\_OF\_FIRM\_SHORT} has day-to-day access to all group client information and records)

It is the responsibility of the UK firm to satisfy itself that the standards of identification are acceptable.

The forms in Annex 5-II attached to the JMLSG may be used for group introduction confirmations.

## Production of Documents

Any Introducer must be able to supply copies of the client due diligence documents to {NAME\_OF\_FIRM\_SHORT} on request. The documentation should be provided within 48 hours unless an extended timeframe is agreed between both parties.

If at any time you become concerned that an introducer is not obtaining sufficient information on clients and or is unable to provide copies of documents on request then this matter must be referred to the MLRO.

# CHAPTER 8: SUSPICIOUS TRANSACTIONS

## Internal Reporting

### Obligation to Report

Every member of {NAME\_OF\_FIRM\_SHORT}’s staff, whether FCA approved or not, is required to make a formal report to the MLRO if, in the course of their employment, they know, suspect, or have reasonable grounds for either knowing or suspecting money laundering or terrorist financing. Reporting in accordance with this requirement will not result in the breach of the Data Protection Act 1998, confidentiality or any other contractual or statutory provisions.

Remember that a duty to report a suspicion of money laundering exists even if a potential client does not conduct any business through {NAME\_OF\_FIRM\_SHORT}, or if we decline the business. The obligation to report is in respect of anyone, whether the firm’s client or not. This is different from the obligation to report fraud that applies to {NAME\_OF\_FIRM\_SHORT}’s actual, and not potential, clients only.

### Objective Test

It is important to understand that a person could be found guilty of a failure to report even if they did not actually suspect but ought to have suspected money laundering. The test is whether an honest and reasonable person, working within the financial services industry, would have formed a suspicion based on the facts available at the time. Generally, to satisfy this test you would have to know your client, their business and the rationale for their instruction, activity or transaction. A failure to make adequate enquiries or assess relevant facts will not provide protection against the objective test of reasonable suspicion.

A suspicious activity or transaction will often be:

### Any transaction or instruction that is not logical from an economic, financial or banking point of view.

### Any transaction where the amount, duration or other specific feature is inconsistent with the customer's professional or business activities, or expected account activity.

**What is meant by reasonable grounds to know or suspect**

Reasonable grounds to know or suspect introduces a negligence test as a deterrent against those in banks and other financial sector banks who fail to act competently, reasonably and honestly where information before them ought to make them suspect money laundering. It may therefore be considered to cover:

### Wilful blindness i.e. turning a blind eye to the obvious.

### Negligence i.e. failing to make adequate enquiries that an honest and reasonable person would be expected to make in the circumstances.

### Failing to assess adequately the facts and information that are either presented or available and that would put an honest and reasonable person on enquiry.

### Timing of Reporting

The obligation is to make a report as soon as reasonably practicable.

### Discharge of Individual Responsibility

By submitting a report to the MLRO you will discharge your individual responsibility under s330 POCA 2002, thus protecting yourself from criminal prosecution for the offence of a failure to disclose. Therefore, when reporting a suspicion, you will receive a formal written acknowledgment from the MLRO. Please retain it for your own records.

### Consultation with a Colleague or Line Manager

It is acceptable to discuss your suspicion with your line manager. However, if after consulting your line manager you remain suspicious, it is your responsibility to ensure that a report is submitted to the MLRO.

While a line manager may comment on the proposed report, they do not have the authority to block or attempt to block any report being made to the MLRO. Should you encounter an attempt to prevent a report being made, you should discuss this with the MLRO directly.

In addition, if you consult a colleague, this colleague will have knowledge on the basis of which they must consider whether or not to make a report to the MLRO. To avoid making duplicate reports, the colleague, if suspicious, should only report if they are reasonably satisfied that the employee will not make such a report.

To reduce the risk of inadvertently tipping off a client the case should be discussed with as few people as possible.

### Continuous Obligation to Report

Making a report does not remove the need to notify the MLRO of further suspicions that may arise with the same or different client. If further suspicions arise additional reports must be made to the MLRO.

### After Submission of a Report

Until the MLRO informs you that no report to NCA is to be made, any further transactions or activity in respect of the suspected client must be reported to the MLRO as soon as they arise.

### MLRO’s Determination

The MLRO will consider the report and surrounding circumstances and decide whether or not to submit an external report to NCA. If the MLRO decides to do so, they must do this as soon as practicable.

In order to undertake this investigation the MLRO may need further information or access to client files. The MLRO must be given free access to all client records. If further information needs to be obtained from the client or from an intermediary then this should normally be obtained by the employee with the client relationship. This is to minimise the risk of alerting the client or intermediary that a disclosure of NCA is being considered.

The MLRO will record all internal enquiries made in relation to the report of a suspicion and the basis for their decision to make or not to make a report to NCA.

A failure to make a report when there are reasonable grounds for a suspicion may constitute assistance under ss.327-329 POCA 2002.

If a disclosure to the MLRO causes them to acquire knowledge or suspicion of money laundering (or gives them reasonable grounds for such knowledge or suspicion) and the MLRO fails to make a report to NCA, then they will be committing the offence of a failure to disclose under s. 331 POCA 2002.

### Pre-Transaction Reporting to NCA

If a pre-transaction report is made by the MLRO to NCA, no business may be conducted with or for a client until you receive consent from NCA. NCA has 7 working days, from the working day following the day of the disclosure, in which to respond to the MLRO. Dealing with or advising a client before receiving consent from NCA may constitute one of the offences under ss.327-329 POCA 2002, that is concealing, arrangements or acquisition, use and possession.

Note there are no provisions under the Terrorism Act for consent to be given within a specified period. If a report is made to SOCS under this Act no related transaction or activity is allowed to proceed until {NAME\_OF\_FIRM\_SHORT} has been contacted by NCA or a law enforcement agency.

The MLRO will inform you whether NCA consents to you dealing with the client or not. Please liaise directly with the MLRO who will provide guidance on what information may be provided to a client or potential client.

### Post-Transaction Reporting to NCA

Since NCA cannot provide consent after a transaction or activity has already occurred, it will provide an acknowledgment of receipt of a report to the MLRO. In the absence of an indication to the contrary from the MLRO, you may deal with the client as normal. However you must inform the MLRO of every interaction with the client and seek guidance on how to deal with that client.

### Contact with Client and Third Parties

Any contact from the client questioning the delay in processing their transaction needs to be handled very carefully. In these circumstances please liaise closely with the MLRO.

Whether or not NCA allows you to proceed with a transaction, you may not tip off the client that a disclosure to the authorities has been made. Neither may you disclose that such a disclosure has been made in response to a data protection request.

Unless specifically authorised to do so, you must not discuss any reports of suspicions of money laundering with third parties. Any requests for information from third parties, such as the Police or Customs, must be immediately referred to the MLRO.

### Court Orders

Any evidence to be presented in Court will be obtained under a court order. The following are the types of order that may be served on {NAME\_OF\_FIRM\_SHORT} as part of an investigation.

* Production order
* Disclosure order
* Customer information order
* Account monitoring order
* Search and seize warrant
* Order for financial information under Terrorism Act

All such orders should be passed to the MLRO immediately who will liaise with {NAME\_OF\_FIRM\_SHORT}’s legal advisers as appropriate.

### Failure to Make a Report

In addition to the sanctions under the POCA 2002, {NAME\_OF\_FIRM\_SHORT} will take disciplinary action against any member of staff who fails to report a suspicion without a reasonable excuse.

### Form of Reporting

Please make your report to the MLRO on the Suspicious Transaction Reporting Form (Money Laundering) attached as Appendix 1. Please give as much information on this form as possible to assist the MLRO.

## Examples of Suspicious Activity

Below is a list of activities that may give rise to a suspicion of money laundering or terrorist financing. This is not an exhaustive list of circumstances; neither will they necessarily give rise to a suspicion. However any of these occurrences is likely to form a basis for further enquiry in most cases. It will be ultimately a matter for your own consideration to decide whether or not to report a suspicion.

* Transactions with no apparent purpose or that make no economic sense
* Transactions of a size or pattern which is out of line with transactions normally undertaken by the client
* The client refuses to provide the information requested
* Accounts that are used for a short period of time only
* Dormant accounts that get reactivated
* Extensive use of offshore vehicles or structures, especially if they do not make economic sense
* Unnecessary routing of funds through third party accounts

## Ongoing Relationships with Suspicious Clients

{NAME\_OF\_FIRM\_SHORT} ’s policy is not to maintain relationships if the firm believes that we may be used for money laundering. Where a client has been involved in a suspicious transaction, the MLRO, together with the senior management, makes a decision regarding the ongoing relationship with that client. If we decide to continue a client relationship, we may implement increased monitoring of the client’s account. Where a client has been the subject of a referral to NCA by the MLRO, the MLRO must be informed before any action is taken to exit the relationship. In such circumstances the MLRO will consult NCA to obtain permission to terminate the client relationship.

## Data Protection – Subject Assess Requests (SARS)

Occasionally a SAR will be received in respect of a client where an internal or external suspicious transaction report has been made. Whilst the Data Protection Act (“DPA”) seeks to ensure all information is included in any response to a SAR request; it does allow, under Section 29 of the DPA, to omit information which may prejudice the prevention or detection of crime. Any such request will need to be handled sensitively and will require the MLRO to liaise with NCA as well as their legal advisers when deciding whether to omit any information. Any decision in respect of the Section 29 exemption must be clearly documented.

## Record Keeping

Under Section 341 POCA it is an offence to destroy any documentation which may be relevant to a money laundering investigation. Records of all internal and external reports together with any supporting documentation must be retained for 5 years from the date of the report. If, however, the firm is aware of an ongoing investigation in relation to any report it must be retained until the relevant agency has confirmed that the case is now closed.

# CHAPTER 9: TRAINING AND AWARENESS

## Introduction

For the purpose of this manual “awareness” refers to actions taken by {NAME\_OF\_FIRM\_SHORT} to ensure that on an ongoing basis personnel are informed of money laundering and associated risks as well as their individual and collective responsibilities.

“Training” refers to a more specific process whereby staff are educated on specific areas, their attendance is recorded and understanding measured.

{NAME\_OF\_FIRM\_SHORT} has a legal responsibility to ensure that personnel receive appropriate anti-money laundering training. Failure to provide training may constitute a criminal offence.

## Awareness

It is our policy to ensure that all employees are aware and kept up to date with money laundering developments. This Handbook serves as the basis for awareness within {NAME\_OF\_FIRM\_SHORT} . It will be supplemented with additional material as and when necessary.

At the start of their employment every employee must be given a copy of this Handbook and must sign an Anti-Money Laundering Handbook Declaration attached as Appendix 6 to confirm that they have read and understood the provisions of this Handbook.

## Training

{NAME\_OF\_FIRM\_SHORT} provides training to relevant staff upon recruitment and on an annual basis. The definition of “relevant staff” is set as widely as possible to encompass all employees who may be able to identify suspicious transactions during the course of their work. The requirement to train relevant staff is also applicable to any part-time, temporary or consulting staff.

Anti- money laundering training will, as a minimum, comprise the following issues:

* The need to obtain sufficient evidence of identity
* Recognition and reporting of suspicions of money laundering via the MLRO to NCA
* The identity and responsibilities of the MLRO
* Anti-money laundering rules, guidance and regulations
* Effects of breaches of money laundering legislation on {NAME\_OF\_FIRM\_SHORT} and its employees

The attendance or completion of anti-money laundering training is mandatory for all relevant personnel. If you are unable to attend on a scheduled training date you should contact the course organiser or provider as soon as possible to arrange an alternative date. Repeated failures to attend training courses may result in disciplinary action.

If, after attending a training course, you feel that you would benefit from further clarification on certain subjects; please contact the MLRO.

## Record Keeping

{NAME\_OF\_FIRM\_SHORT} will retain the records of all materials issued to its personnel in relation to anti money laundering training and awareness for at least 5 years from the date of issue of materials.

These records will include the names of attendees, dates of all training sessions, content of courses and presentations and, where applicable, tests results. All staff will be required to sign the Register of Attendees attached as Appendix 2 confirming that they have received training and understood their legal responsibilities.

# CHAPTER 10: MONITORING JMLSG 5, ML 7.2

## Introduction

Due to {NAME\_OF\_FIRM\_SHORT}’s size and nature of its business, the firm, in monitoring clients’ activities, places reliance on two main factors:

1. Having up-to-date client information; and
2. Asking pertinent questions to elicit the reasons for unusual transactions

## Up-To-Date Client Information

We ensure that the information we keep about our clients is up-to-date through regularly performing client reviews. The frequency of such reviews is determined by the client’s risk category. Apart from the transaction monitoring on each account, we review our clients with the following frequency: *(amend as required)*

* Low risk clients are re-assessed every 3/4/5 years
* Medium risk clients are re-assessed every 2/3 years
* High risk clients are re-assessed at least annually/six monthly
* PEPs are re-assessed quarterly/six monthly

The purpose of these reviews is to identify any significant changes to the corporate structure, management and activities of the client. Unless the MLRO resolves otherwise, it is not always necessary to obtain all the information required for account opening or to re-verify all identification information. These reviews are coordinated by the MLRO. In addition to reviewing changes to the client’s structure, management and profile an overall review of the client’s activity over the period is normally conducted. This will allow {NAME\_OF\_FIRM\_SHORT} to assess if there have been changes in the client’s activity which could be considered unusual given the information held about the client.

Notwithstanding these timescales, should any member of staff become aware of a change in the circumstances of a client, for example change of ownership structure or move into a new business area, this information should be recorded on the client file immediately. If this information could affect the risk assessment of the client then the MLRO should be informed. The MLRO will then decide if there is the need to re-evaluate the client’s risk assessment.

## Transaction Monitoring

We consider that a combination of anti-money laundering training and commercial awareness will enable our staff to monitor for, recognise and report suspicious activities.

We will seek to understand the rationale for the client undertaking a particular transaction or activity. When identifying unusual or potentially suspicious activity our staff will use their knowledge of the client and of what would be normal in a given set of circumstances.

In general terms, all members of staff should have regard to the following considerations when monitoring client accounts, as well as factors detailed in other chapters of this Handbook:

* Whether the financial performance of an enterprise is in line with the nature and scale of its business, and whether the corporate finance services it seeks appear legitimate in the context of those activities.
* The unusual nature of a transaction: e.g., abnormal size or frequency for that client or type of client
* The nature of a series of transactions: for example, a number of cash payments
* The geographic destination or origin of a payment: for example, to or from a high risk jurisdiction
* The parties concerned: for example, a request to make a payment to or from a person on a HM Treasury Sanctions List attached as Appendix 5.

However {NAME\_OF\_FIRM\_SHORT} recognises that while staff training is important, it is not a comprehensive substitute for transaction monitoring. Therefore, on a quarterly basis {NAME\_OF\_FIRM\_SHORT} will formally review all transactions undertaken each quarter to ensure that no money laundering has been facilitated or taken place.

Please refer to the Post-Transaction Review Form contained in Appendix 7 to this Handbook.

## Record Keeping

Evidence of all monitoring undertaking by {NAME\_OF\_FIRM\_SHORT} will be retained for a period of at least 5 years from the date of the review.

# CHAPTER 11: RECORD RETENTION

## Introduction

This chapter provides guidance on the record keeping procedures that {NAME\_OF\_FIRM\_SHORT} needs to meet their obligations in respect of the prevention of money laundering and terrorist financing.

Keeping adequate records will ensure that {NAME\_OF\_FIRM\_SHORT} can:

* Provide an audit trail for all advice given and activity undertaken on a client’s behalf
* Provide adequate information to the law enforcement agencies to assist with their investigations
* Undertake monitoring of client activity against expectations
* Identify and report any suspicious activity
* Provide evidence of meeting all statutory and regulatory obligations

## What records have to be kept?

The following material must be kept:

* Client information, including evidence of identify
* Details of all transactions made on behalf of each client
* Internal and external reports of suspicion
* MLRO annual report and any other reports
* Information not acted upon
* Training and compliance monitoring
* Information about the effectiveness of training

Keeping the required records for the specified time period will not result in {NAME\_OF\_FIRM\_SHORT} breaching the Data Protection Act 1998. This information will be made available to the competent authorities in the context of any relevant criminal investigations and prosecutions.

## Identification Records

Client identification records must be kept for a period of at least 5 years from the date of the end of a client relationship. That is either the date of last transaction with the client or the closure of client account, whichever is the latest.

## Transaction Records

Transaction records must be kept for a period of at least 5 years from the date of the transaction. They should be maintained in a form which provides satisfactory audit trail of all transactions effected via {NAME\_OF\_FIRM\_SHORT} allowing their reconstruction.

## Third party Record Keeping

If {NAME\_OF\_FIRM\_SHORT} has an appointed representative, then it is {NAME\_OF\_FIRM\_SHORT}’s responsibility to ensure the representative complies with the record keeping obligations. This principle also applies to the use of third party service providers such as introducers or administrators.

## Internal and External Suspicious Transaction Reports

We will retain the following records of any reports of suspicions of money laundering regardless of whether the MLRO made a report to NCA. These records will consist of:

* Records of actions taken under the internal and external reporting requirements
* When the MLRO had reviewed an internal report and decided not to make a report to NCA, a record of all the information considered
* Copies of reports of suspicions submitted to NCA

These records will be retained for 5 years from the date the report is made. However, if {NAME\_OF\_FIRM\_SHORT} is aware that either NCA or another law enforcement agency is conducting an investigation into a client, {NAME\_OF\_FIRM\_SHORT} will retain all records in relation to that client until the agency confirms that the case is closed. If, within 5 years of a disclosure being made, {NAME\_OF\_FIRM\_SHORT} has not been advised of an ongoing investigation, it may destroy the records.

## Anti-Money Laundering Training Records

We will retain the following records for at least 5 years in relation to Anti-Money Laundering (“AML”) training:

* Date(s) AML training was given
* Nature and content of the training
* Names of people who received the training
* The results of the tests taken, if applicable

## Compliance Monitoring Records

The following records are retained for at least 5 years in relation to compliance monitoring:

* Annual MLRO report to the board and any other reports to senior management
* Records of consideration of those reports and of any action taken as a consequence

## Refused Business Records

Where business has been refused because it does not meet our client identification, verification and KYC standards, a record of the refusal will be retained for 5 years.

## Wire Transfer and Electronic Payment Records

All electronic payment messages should contain sufficient information to identify the parties involved (i.e. both the party making the payment and the beneficiary). This information should include full names, addresses and account numbers. Where this information cannot be provided in the electronic payment message, full records must be retained.

## Format and Retrieval of Records

{NAME\_OF\_FIRM\_SHORT} aims to reduce the volume and density of records. While still complying with the statutory requirements we may choose to keep records:

* By way of original documents
* By way of photocopies of original documents
* On microfiche
* In scanned form
* In computerised or electronic form

{NAME\_OF\_FIRM\_SHORT} may keep records either offsite or outside the UK, but will remain responsible for ensuring that all required records can be made available without undue delay and meet the UK regulatory requirements. {NAME\_OF\_FIRM\_SHORT} will ensure that all records, however kept, are capable of being retrieved within 48 hours. {NAME\_OF\_FIRM\_SHORT} will, whenever possible, seek to retain all records on the business premises.

## Sanctions and Penalties

Where a firm fails to observe the record keeping requirements either the firm, or relevant person(s) or both are open to prosecution. This may include imprisonment for up to 2 years, an unlimited fine and/or regulatory censure.

# Appendix 1: Suspicious Transaction/Activity Reporting Form (Money Laundering)

Name of Person Reporting a Suspicion

Job Title or Responsibility

**BUSINESS/CORPORATE CUSTOMER**

**Account Number (if applicable)**

Company Name: ………………………………………………………………………….…………..

Address: ………………………………………………………………………………………………

Contact/Tel: …………………………………. Nature of Business………………………………..

**PERSONAL CUSTOMER**

**Account Number (if applicable)**

Name: …………………………………………………………………………………………………..

Address: ………………………………………………………………………………………………

Contact/Tel: ……………………………………….. Occupation/Employer: ………………….

Passport No: ………………………………………. Nationality: ………………………………

Other ID: …………………………………………. Date of Birth: ……………………………

Other Verification Evidence:

(if applicable) …………………………………………………………………………………………..

**CONNECTED ACCOUNTS (please provide account name, number and the nature of the relationship)** ……………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………

Details of Event(s) Giving Rise to a Suspicion (use a separate sheet of paper if necessary)

Details of Supporting Evidence Attached (if any)

This report is being made **PRE** or **POST** transaction (delete as applicable)

A separate sheet of paper is attached (tick if applicable)

Signed

Dated

**ONCE COMPLETED PLEASE PASS THIS FORM TO THE MLRO OR DEPUTY MLRO IMMEDIATELY. PLEASE RETAIN A COPY OF THIS REPORT FOR YOUR OWN RECORDS.**

**END OF STAFF REPORT**

**To be completed by the MLRO**

Client name

Date Received

Date Review Completed

Comments Regarding the Suspicion

|  |
| --- |
| I have reviewed the report and have concluded; |

**Reported to NCA?**

**Yes** copy of NCA report attached.

If disclosure is prior to an event, have the appropriate measures been taken to ensure the transaction cannot proceed for the next 7 working days?

|  |
| --- |
| I have decided that the suitable action is; |

**No** basis for non-disclosure is included in comments above

Signed

Position **MLRO / DMLRO**

Dated

**MLRO USE:**

NBE Reference……….

Date received: ………….. Time received: ……………

**Pre-advised activity consent report?** ……………….. **Yes / No**

NCA advised? Yes/No Date:…….. ……………….Time:…………………..

NCA Reference: …….…………….

NCA consent received/denied/assumed………………Date:……………………

# Appendix 2: Register of Attendees

**DATE:**

**COURSE TOPIC:** AML TRAINING INCLUDING PERSONAL LEGAL OBLIGATIONS

**PLEASE SIGN BELOW TO CONFIRM YOU HAVE ATTENDED THE ABOVE TRAINING COURSE AND HAVE UNDERSTOOD THE CONTENT COVERED.**

|  |  |
| --- | --- |
| **NAME** | **SIGNATURE** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**PLEASE KEEP THIS REGISTER ON FILE WITH A COPY OF THE PRESENTATION AND COURSE MATERIALS.**

# Appendix 3: New Account Opening Form (“NAO”) *[Amend as required]*

|  |
| --- |
|  |

|  |  |
| --- | --- |
| **Client Name** |  |
| **Nature of Business Relationship** |  |
| **Purpose** | **New Account /Review** |
| **Risk Rating** | **PEP/ High/ Medium/ Low** |
| **Risk Assessed PEP?** | **Yes / No** |
| **Due Diligence Level** | **Enhanced/ Simplified/ Normal** |
| **Date of Review** |  |
| **Next Review Date** |  |
| **MLRO Sign-off Date [if required]** |  |
| **Summary** (include relevant information on PEPs, adverse media, etc) |  |

|  |  |
| --- | --- |
| **{NAME\_OF\_FIRM\_SHORT} NEW CLIENT ACCOUNT OPENING FORM** | |
| 1. **CLIENT INFORMATION** | |
| **Reference Number** |  |
| **Date of Instruction** |  |
| **Full Legal Name:** |  |
| **Trading name (if different)** |  |
| **Address of Principal place of Business** |  |
| **Registered address** |  |
| **Registered number** |  |
| **Website (if any)** |  |
| **Legal Entity Identifier (LEI) (as applicable)** |  |
|  |  |
| **2.CLIENT’S REPRESENTATIVE DETAILS [3rd party or intra-group]** | |
| **{NAME\_OF\_FIRM\_SHORT} Account Manager** |  |
| **Name of contact** |  |
| **Position in Firm** |  |
| **Approach (face-to-face, email/Internet, other?)** |  |
| **Is contact known to firm/bank/company?** |  |
| **How long?   *- Relationship with bank is 1 year or less  - Relationship with bank is 2 - 4 years  - Relationship with bank over 5 years*** |  |
| **How have you satisfied yourself that the individual has the authority to represent the firm? Please specify below (Proof of Authority on file, eg, authorised signatories list)** |  |
| **Telephone** |  |
| **Facsimile** |  |
| **Email address/es** |  |
| **Organisation Chart – Company/Group?** |  |
| **BUSINESS TYPE** | |
| Please provide a brief description on the client. | |
| Please provide details of the nature, size and frequency of business activity anticipated with this client  **Type of activity**   |  |  |  | | --- | --- | --- | | Buying products/services □ | Providing products/services □ | Not applicable □ |  |  |  | | --- | --- | | Money Market | □ | | FX | □ | | Clearing bank | □ | | Counterparty for trading Investment Bonds | □ | | Trade Finance | □ | | Current Account Services | □ | | Other | □ |   Please state …………………………………….. | |
| **REQUIRED BUSINESS TYPE** | |
| **Type of Service or Product to be provided** | |
|  | |

**SECTION A1 CUSTOMER CLASSIFICATION**

**Eligible Counterparty (only in respect of eligible counterparty business)**

Please tick as appropriate

|  |  |
| --- | --- |
|  | **Evidence attached** |
| * Investment firms |  |
| * Credit institutions |  |
| * Insurance companies |  |
| * C[ollective investment scheme](http://fsahandbook.info/FSA/glossary-html/handbook/Glossary/C?definition=G178)s authorised under the [UCITS Directive](http://fsahandbook.info/FSA/glossary-html/handbook/Glossary/U?definition=G1199) or their management companies |  |
| * Pension funds and their management companies |  |
| * other financial institutions authorised or regulated under European Community legislation or the national law of an [EEA State](http://fsahandbook.info/FSA/glossary-html/handbook/Glossary/E?definition=G329) (including includes regulated institutions in the securities, banking and insurance sectors) |  |
| * undertakings exempted from the application of MiFID under either Article 2(1)(k) (certain own account dealers in commodities or commodity derivatives) or Article 2(1)(l) (locals) of that directive |  |
| * National and regional governments, public bodies that manage public debt, central banks and international and supranational institutions |  |
| * central banks |  |
| * supranational organisations |  |

**Attach evidence to support categorisation.**

If any box above ticked; proceed to section B

If **none** of the boxes above are ticked; proceed to **section A2**.

**Eligible Counterparty Business**

Eligible Counterparty Business consists of the following services and activities carried on by a firm:

1. dealing on own account, execution of orders on behalf of clients or reception and transmission of orders; or
2. any ancillary service directly related to a service or activity referred to in (a); or
3. arranging in relation to business which is not MiFID or equivalent third country firm business;

but only to the extent that the service or activity is carried on with or for an eligible counterparty.

**SECTION A2 CUSTOMER CLASSIFICATION**

**“Per Se” Professional Client**

Please tick as appropriate:

|  |  |
| --- | --- |
|  | **Evidence attached** |
| Entities required to be authorised or regulated to operate in the financial markets: |  |
| * Credit institutions |  |
| * Investment firms |  |
| * Other authorised or regulated financial institutions |  |
| * Insurance companies |  |
| * Collective investment schemes and their management companies |  |
| * Pension funds and their management companies |  |
| * Commodity and commodity derivative dealers |  |
| * Locals |  |
| * Other institutional investors |  |
| Large undertakings meeting two of the following size requirements on a company basis:   * Balance sheet total of €20m * Net turnover of €40m * Own funds of €2m |  |
| National and regional governments, public bodies that manage public debt, central banks and international and supranational institutions |  |
| Other institutional investors whose main activity is to invest in financial instruments, including entities dedicated to the securitisation of assets or other financing transactions |  |

**Attach evidence to support categorisation.**

If any box above ticked; ticked proceed to section B

If **none** of the boxes above are ticked; proceed to **section A3.**

**SECTION A3 CUSTOMER CLASSIFICATION**

**Retail Clients Requesting Treatment as ‘Elective’ Professional Clients (Opt-Up)**

**Has the client requested to be opted up to be an “elective” professional client.**

Yes □ Proceed to Qualitative test

No □ The client is a Retail Client

**The request to opt up must come from the client and not from the firm.**

Qualitative Test A3a

{NAME\_OF\_FIRM\_SHORT} has reviewed the client’s expertise, experience and knowledge and we believe the client is capable of making his own investment decisions and understanding the risks involved. If the client is an entity, the qualitative test should be performed in relation to the person authorised to carry out transactions on its behalf.

Reasoning

………………………………………………………...……………………………………………………………

………………………………………………………...……………………………………………………………

………………………………………………………...……………………………………………………………

………………………………………………………...……………………………………………………………

Quantitative Test A3b

The client must satisfy at least two of the following: Tick box and supply supporting documentation

|  |  |
| --- | --- |
| the client has carried out transactions, in significant size, on the relevant market at an average frequency of 10 per quarter over the previous four quarters |  |
| the size of the client’s financial instrument portfolio, defined as including cash deposits and financial instruments, exceeds €500,000 |  |
| the client works or has worked in the financial sector for at least one year in a professional position which requires knowledge of the transactions or services envisaged. |  |

Reasoning and evidence

………………………………………………………...……………………………………………………………

………………………………………………………...……………………………………………………………

………………………………………………………...……………………………………………………………

………………………………………………………...……………………………………………………………

………………………………………………………...……………………………………………………………

**If the client does not fall to be an eligible counterparty, per se professional client or “elective” professional client, the client will be a Retail Client.**

**In completing the form below – it is required to identify all areas that may reflect the client’s status or the bank’s experience in dealing with that client. Whilst there is the option for the MLRO to decide on a lower rating, it is your responsibility to defer to the higher rating on all categories, whether Legal Entity, Geographical or Industry Risk. Product Risk is monitored and decided by Treasury/Investment Committee (if applicable) and the Board regarding Investment Practices.**

**The form below reflects the three risks mentioned, specifically H6 to H11 for higher risk categories.**

**Complete ALL PEP details (if identified) in B2 Box 6**

**Boxes are designed to acknowledge the actions taken, with details entered in the “Notes” Boxes below each section.**

**SECTION B1 AML RISK ASSESSMENT**

| **Low Risk** | **Tick** | **Medium Risk** | **Tick** | **High Risk** | **Tick** |
| --- | --- | --- | --- | --- | --- |
| L1. Regulated financial institutions based in the UK; EU, or comparable jurisdiction. |  | M1. Private companies based in the UK, EU or comparable jurisdiction provided they are not undertaking high risk business activities |  | H1. Relationships where a Politically Exposed Person (“PEP”) or their connected person has been identified as having significant involvement. |  |
| L2. UK Public authorities or community institutions. |  | M2. Low risk clients whose identification documents cannot be independently verified |  | H2. Relationships involving clients residing in or nationals of Non-FATF Countries |  |
| L3. Companies or their subsidiaries (50% or more) whose shares are traded on an EU regulated market or equivalent exchange. |  | M3. Subsidiaries of or entities associated with low-risk clients |  | H3. Accounts that involve regular payments to or from unrelated third parties |  |
| FOR CATEGORIES L1 TO L3 ABOVE REFER TO section B2 BOX 1 |  | M4. All other clients that do not fall within either a low risk category or a high risk category |  | H4. Complex business ownership structures, such as offshore special purpose vehicles, that make it easier to conceal underlying beneficiaries, especially where there is no legitimate commercial rationale |  |
| L4. Clients represented by those whose appointment is subject to court approval or ratifications (e.g. executors) |  | *Not Applicable* |  | H5. Names that have been previously linked with financial crime |  |
| L5. Non UK Government offices and agencies in all jurisdictions except for those in the Non-FATF Countries. |  | *Not Applicable* |  | H6. Clients based in or conducting business in or through a high-risk jurisdiction with known level of corruption, organised crime, or drug production and distribution. Further details relating to corruption and indices of country’s ratings can be found on the Transparency International lists. (www.transparency.org). See Appendix 8 for the latest list. [{NAME\_OF\_FIRM\_SHORT} to decide cuttoff] |  |
| L6. Firms in UK that are members of a recognized professional body (for example, Law Society or ICAEW) |  | *Not Applicable* |  | H7. Clients engaged in a business that involves significant amounts of cash or higher risk business activities (e.g. arms dealing) |  |
| *Not Applicable* |  | *Not Applicable* |  | H8. non-face to face clients **except for low risk clients** |  |
| *Not Applicable* |  | *Not Applicable* |  | H9. Companies issuing bearer shares, especially if incorporated in high-risk jurisdictions |  |
| *Not Applicable* |  | *Not Applicable* |  | H10. Clients previous the subject of a Suspicious Transaction Report |  |
| *Not Applicable* |  | *Not Applicable* |  | H11. Trusts with complex structures or that are based in or financially linked to higher risk jurisdictions. Includes Charities. |  |
| **FOR CATEGORIES 4 & 5 ABOVE REFER TO THE MLRO** |  | **FOR MEDIUM RISK CLIENTS REFER TO SECTION B2 - BOXES 2, 3,4 AND 5** |  | **FOR HIGH RISK CLIENTS REFER TO SECTION B2 - BOXES 2, 3, 4 & 5** |  |

**Please choose the category to which the client belongs and tick appropriate box, then follow relevant guidance. Where a client fits in one or more categories the MLRO should determine the rating and reasoning for rating.**

**SECTION B2 IDENTIFICATION AND VERIFICATION**

|  |
| --- |
| **BOX 1 – LOW RISK CLIENTS SUBJECT TO SIMPLIFIED DUE DILIGENCE**   1. A company listed on an EU regulated market or equivalent exchange., 2. or whose parent is listed on such an exchange ………………………………………………………..□  Provide name of the exchange: ………………………………………………………………………………   If a subsidiary of the listed company, please state percentage owned by  listed parent. …………………………..  2. A UK public authority or community institution □  3. A regulated financial institution located in a UK, EU or □  equivalent jurisdiction acting either as a principal or as an agent  Name of regulator:  Regulatory firm reference number:  **Verification**  *Please attach evidence from an independent source e.g. exchange or regulator’s website (containing both the name* ***and*** *address of the client). If the exchange is not an EU regulated market provide rationale/contemporary evidence as to it equivalence.* |
| **Notes for Section B2 Box 1**  **Please complete as appropriate *(box will expand as you type)*** |

|  |
| --- |
| **BOX 2 – MEDIUM or HIGH RISK FINANCIAL INSTITUTIONS**  1. A **regulated financial institution** not falling under Section B2 Box 1 part 3 acting as either:  a) principal; or …………………………………………………….□  b) an agent ………………………………………………………..□  *Identify the financial institution in accordance with identification requirements for private companies, limited partnerships or unincorporated associations or public companies in non-equivalent jurisdictions, whichever is applicable. Boxes 3, 4 & 5.*  *If acting as an agent, you need to identify the underlying principal and a new form needs to be completed for that person.*  **CARE SHOULD BE TAKEN**  **When screening High-Risk & Pep Customers**. There are legitimate uses for offshore companies and trusts. A “hit” does not intend to suggest or imply that any people, companies or other entities included in the ICIJ Offshore Leaks Database have broken the law or otherwise acted improperly. Many people and entities have the same or similar names. You should confirm the identities of any individuals or entities located in the database based on addresses or other identifiable information |
| **Notes for Section B2 Box 2**  **Please complete as appropriate *(box will expand as you type)*** |

|  |
| --- |
| **BOX 3 – PRIVATE or PUBLIC COMPANIES or equivalent**  Medium risk companies listed on UK/EEA/EU regulated market or equivalent exchange or regulated financial institutions based in the UK/EU, or equivalent jurisdiction (e.g. where higher risk indicators such as PEPs requires application of greater due diligence)  Companies not listed on an EU regulated market or equivalent UK/EEA exchange.  **OBTAIN THE FOLLOWING ID INFORMATION**  *Please seek to obtain this evidence from independent sources.*  1. Evidence of the client’s full **name and registered number**:  A copy of Certificate of Incorporation; or □  Companies House (Credit Reference, Banks   Reference or equivalent registry) search □  Memorandum & Articles of Association □  2. Evidence of client’s **registered office** in the country of its incorporation:  A confirmation of the address by a reputable professional person; or □  Companies House (or equivalent registry) search □  Other □  3. Evidence of client’s **business address**:  A copy of a utility bill; or □  A government issued document; or □  A record of visit to the client’s place of business □  Other □  4. Full Names of all **Directors** □  Number of Directors … (same number of supplementary forms required Box 7)  5. Names of all direct and indirect beneficial owners holding 10% or more  of issued share capital or voting rights (e.g. an ownership chart) □  Number of Shareholders 10%+ … (same number of supplementary forms required)  6. Copy of the latest annual accounts (if available) if not – explain. □  7. FATCA Status [(Check Here) Input GIIN Number:](https://www.irs.gov/businesses/corporations/fatca-online-registration-system-and-ffi-list-giin-composition-information) □  8. Source of Funds evidenced? □  9. If High Risk - Source of Wealth evidenced? □  **Verification**  Verify the identity of all beneficial owners owning or controlling 10% or more of the company and at least one principal director in accordance with the individual requirements in Section B2 - Box 7. |
| **Notes for Section B2 Box 3**  **Please complete as appropriate *(box will expand as you type)*** |

|  |
| --- |
| **BOX 4 - PARTNERSHIPS**   1. A **partnership** □   2. Other **incorporated association** □  Please specify  *Note Scottish Partnerships, limited partnerships and limited liability partnerships should be treated as private companies.*  **OBTAIN THE FOLLOWING INFORMATION**  1. Evidence of trading address □  2. Verification of the nature of business activities □  3. List of all partners (if too many, those of over 25% or more  (10% or more for medium and high-risk clients)) □  Enter all names below – box will expand to accommodate  4. Copy of Partnership agreement □  5.Copy of latest audited accounts (if available) if not – explain. □  6.FATCA Status [(Check Here) Input GIIN Number](https://www.irs.gov/businesses/corporations/fatca-online-registration-system-and-ffi-list-giin-composition-information) |
| **Partners Names (if needed) *Please continue numbering as appropriate.***  **1**  **2**  **3**  **4**  **…..** |
| **Verification**  Verify the identity of all partners owning or controlling 10% or more of the partnership in accordance with the individual requirements in Section B2 Box 7.  If clients are medium risk, then there is only a requirement to identify the most senior member of the governing body. If client is high risk, all need to be ID&V’d.  *Please consult your MLRO to determine the need for further verification checks.* |
| **Notes for Section B2 Box 4**  **Please complete as appropriate *(box will expand as you type)*** |

|  |
| --- |
| **BOX 5 – SCREENING**   1. Screening on client □ 2. Screening on Directors, Partners or equivalent □ 3. Screening on direct and indirect beneficial owners holding 10% or more of Issued share capital or voting rights □ 4. Any adverse media screening (please specify below) □ 5. World-Check (Thomson Reuters) □ 6. Panama Papers ICIJ Database □ |
| **Notes for Section B2 Box 5**  **Please complete as appropriate *(box will expand as you type)*** |

|  |
| --- |
| **BOX 6 - ADDITIONAL INFORMATION FOR PEPs**  **Identified PEP Numbers?** □  **Names of PEP;**  **Names of PEP;**  **Names of PEP;**  **Names of PEP;**  **Names of PEP;**  **Names of PEP;**  Explanation of Why this person/these people have been identified as PEPs;  Source of Wealth and Source of Funds are completed and attached to the Individuals Section (Box 7 – *one per person*)  We have managed the PEP by;   * Measures in line with {NAME\_OF\_FIRM\_SHORT}’s PEP policy. * Senior Management has approved the PEP policy mandating a proportionate PEP approach in accordance With MLR 2017 Regulation 33(2)(c). However, if there any adverse media occurs at any time, then full EDD will be applied.   **NOTE:** In respect of PEPs the source or wealth and/or source of funds needs to be documented and the General Manager is required to countersign the New Account Form.  **TO BE SIGNED BY MLRO**  Name  Signature  Date  1. In respect of individuals who have not been met face to face then further documentation or evidence is required (see Section B2 box 7)  If any of the client’s directors or partners have already been identified by {NAME\_OF\_FIRM\_SHORT} please provide details (e.g. reference to a file with the individual’s ID documents):  *Please note that it is your responsibility to ensure that the individual has been properly identified.* |
| **Notes for Section B2 Box 6**  **Please complete as appropriate *(box will expand as you type)*** |

As the **Individuals Box** May be required to be duplicated for each individual identified or required, it has been allocated its own page/s below.

**Duplication Process**

Click Anywhere in box 7

At the top left click on the cross that appears just outside the box.

Copy (right click and select copy or use CTRL+C)

Move cursor to bottom of box and press “Enter” to make a one line gap <IMPORTANT>

Paste (right click and select “paste” or use CTRL+V

|  |
| --- |
| **BOX 7 - INDIVIDUALS**  For individuals **met face-to-face by a member of {NAME\_OF\_FIRM\_SHORT} staff**, detail the following information  Full name  Any Previous names …………………………………………… Date changed ……..  Residential address    Date of birth  **1.** Obtain at least **one** of the following documents containing the subject’s full name and photograph; and either their residential address or their date of birth  a. A **Passport** (must contain the individual’s photo) □  b. A **Driving license** (must contain the individual’s photo) □  c. A **National identity card** (must contain the individual’s photo) □  **2.** If the **above mentioned document is** **not available**, obtain:  a. Government-issued document (can be without a photograph) with the client’s name; AND  b. Second document, either government-issued, or issued by a judicial authority, public sector body or authority, or another regulated firm (by FCA or a regulator in an equivalent jurisdiction) containing the subject’s name; and either their Address OR Birthdate,  **3.** If the client is accepted on a **non-face-to-face basis**, you must obtain one document from List 1 above AND a second document, whether from List 1 or 2 above.  **Please note that mobile phone bills cannot be used to verify identity.**  **Government-issued documents with a photograph include, but are not restricted to:**  Valid passport □  Valid photocard driving licence (full or provisional) □  National Identity card (non-UK nationals) □  Firearms certificate or shotgun licence □  Identity card issued by the Electoral Office for Northern Ireland □  **Government-issued documents without a photograph include, but are not restricted t**o:  Valid (old style) full UK driving licence □  Recent evidence of entitlement to a state or local authority funded benefit  (including housing benefit and council tax benefit), tax credit, pension,  educational or other grant □  **Other documents include, but are not restricted to:**  Instrument of a court appointment (such as liquidator, or grant of probate) □  Current council tax demand letter, or statement □  Current bank statements, or credit/debit card statements, issued by a regulated  financial sector firm in the UK, EU or equivalent jurisdiction (but not ones  printed off the internet) □  Utility bills (but not ones printed off the internet) □  W8 BEN E (complete date etc in notes below) □ |
| **Notes for Section B2 Box 7**  **Please complete as appropriate *(box will expand as you type)*** |

**SUPPLEMENTARY**

**FATCA (USA and UK) and other screening requirements**

|  |  |
| --- | --- |
| Is there any indication that the account holder is a USA Person, Citizen, Resident etc.? If so, ensure that the details are captured.  **NB** Ensure nationality, residence and DOB etc. are recorded below: |  |
| Beneficial Owners:  Declaration |  |
| ICIJ Database – Panama Papers Check |  |
| Residence |  |
| Country of residence for tax purposes |  |
| Any other country mentioned as possible tax domicile? Dual Nationality? Any reference to other countries? Consider and note for FATCA or similar requirements. |  |

**SECTION C DEPARTMENTAL APPROVEMENT**

|  |  |
| --- | --- |
| KYC Analyst Name |  |
| I can confirm all the due diligence has been completed. | **Yes / No** |
| Notes | |
| Confirmed as Acceptable |  |
| Department Manager Name |  |
| Department |  |
| Date |  |

**TO BE COMPLETED BY THE COMPLIANCE OFFICER/ MLRO:**

|  |  |
| --- | --- |
| Customer Classification: | **SECTION A**  Eligible Counterparty □  “Per Se” Professional Client □  “Elective” Professional Client □  Retail □ |
| Documentation, including notification of categorisation sent? | Yes □ |
|  |  |
| Money Laundering Identification and Verification: | **SECTION B**  Sufficient Evidence obtained □ |
| AML Risk Assessment Category Applied to client | High □  Medium □  Low □ |
| Consideration of Conflicts | No conflicts with business or clients □  Potential conflicts identified □  Provide information on any potential conflicts and how they are to be managed/disclosed. |
| Is Client acting as agent?  If yes is underlying principal disclosed or undisclosed | Yes / No  **Disclosed** / **Undisclosed** |
| Compliance Office / MLRO Name |  |
| Signature |  |
| Date |  |

# Appendix 4: Documents for Individuals

This is a non-exhaustive list of documents that may be acceptable when identifying **a private individual:**

**Government-issued documents with a photograph** include, but are not restricted to**:**

* Valid passport
* Valid photocard driving licence (full or provisional)
* National Identity card (non-UK nationals)
* Firearms certificate or shotgun licence
* Identity card issued by the Electoral Office for Northern Ireland

**Government-issued documents without a photograph** include, but are not restricted to**:**

* Valid (old style) full UK driving licence
* Recent evidence of entitlement to a state or local authority funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant

**Other documents** include, but are not restricted to**:**

* Instrument of a court appointment (such as liquidator, or grant of probate)
* Current council tax demand letter, or statement
* Current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK, EU or comparable jurisdiction (but not ones printed off the internet)
* Utility bills (but not ones printed off the internet)

# Appendix 5: Useful Information Sources

**Serious Organised Crime Agency (NCA)**

[www.NCA.gov.uk](http://www.soca.gov.uk)

**NCA Disclosure Form**

NCA has prepared a standard disclosure form. Both this form and guidance on completing it are available at [www.NCA.gov.uk/financialIntel/disclosure.html#forms](http://www.soca.gov.uk/financialIntel/disclosure.html#forms).. NCA prefers reports to be delivered electronically and the details of how to register can be found at <https://www.ukciu.gov.uk/saronline.aspx>.

**List of Regulators**

<http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=773&menu=expand>

**Home Office Proscribed Organisations List**

<http://www.homeoffice.gov.uk/security/terrorism-and-the-law/terrorism-act/proscribed-groups?version=1>

**HM Treasury Sanctions List**

<http://www.hm-treasury.gov.uk/documents/financial_services/sanctions/fin_sanctions_index.cfm>

**Worldwide Registries (Companies House equivalents)** <http://www.companieshouse.gov.uk/links/introduction.shtml>

**Professional Bodies**

<http://www.companieshouse.gov.uk/links/introduction.shtml>

**Comparable Jurisdictions**

Comparable jurisdictions can be summarised as the following:

* EU Member States including Gibraltar as part of the UK, and Netherlands Antilles and Aruba as part of the Kingdom of the Netherlands,
* EEA Countries
* UK Crown Dependencies
* Non-UK FATF Members

It does not exempt {NAME\_OF\_FIRM\_SHORT} from performing wider due diligence and Know Your Customer checks. Neither the “comparability” status provides an exemption from the objective test in the Proceeds of Crime Act 2002. “Comparability” indicates that client identification procedures exist in a country. This is based on the provisions of the legislation in a particular jurisdiction, rather than what actually happens in practice. This applies to both EU Member States and non-EU countries which are "comparable jurisdictions".

<http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=770&a=9814>

**Financial Action Task Force**

The inter-governmental body known as the ‘Financial Action Task Force’ (“FAFT”)’ was established to develop and promote policies, both at national and international levels on combating money laundering and terrorist financing. FATF member countries have committed themselves to implementing the FATF Forty Recommendations which in several respects are more wide-ranging in nature than the provisions of the European Money Laundering Directives. Membership of this inter-governmental body is subject to ongoing approval and monitoring.

[www.fatf-gafi.org](http://www.fatf-gafi.org)

**FATF Member Countries**

<http://www.fatf-gafi.org/document/52/0,3343,en_32250379_32237295_34027188_1_1_1_1,00.html>

**Non-Cooperative Countries and Territories (NCCTs)**

The current list of countries and territories that are not cooperative in the international fight against money laundering can be found on the following website.

<http://www.fatf-gafi.org/document/4/0,2340,en_32250379_32236992_33916420_1_1_1_1,00.html>

Recognised Investment Exchanges, Recognised Overseas Investment Exchanges, Recognised Clearing Houses, Recognised Overseas Clearing Houses, Designated Investment Exchanges and Regulated Markets

[http://www.FCA.gov.uk/register/exchanges.do](http://www.fsa.gov.uk/register/exchanges.do)

# Appendix 6: Anti-Money Laundering Handbook Declaration

1. I hereby acknowledge that I have read and understood the provisions of the {NAME\_OF\_FIRM\_SHORT} ’s Anti-Money Laundering Handbook (“Handbook”).
2. I agree to comply with the policies and procedures of the Handbook. If I am ever unsure about any of the areas covered in this Handbook I will consult {NAME\_OF\_FIRM\_SHORT} ’s Compliance Officer or Money Laundering Reporting Officer.
3. I understand that a breach of any of the provisions of the Handbook may result in criminal prosecution, regulatory censure or disciplinary action by {NAME\_OF\_FIRM\_SHORT} .

Name

Signature

Date

# Appendix 7: Post-Transaction Review Form

Year:

Quarter:

I acknowledge that during the past quarter:

EITHER

□

No accepted, declined or potential business done with of for clients or potential clients of {NAME\_OF\_FIRM\_SHORT} has given rise to a reasonable suspicion of money laundering, terrorist financing or fraud. In making this assessment I have considered all information which is or has become available to me before, after or at the time of any such business.

OR

□

I have carefully reviewed suspicious activity reports submitted to me by {NAME\_OF\_FIRM\_SHORT} ’s staff and either made a formal report to the Serious Organised Crime Agency; or documented my reasons for not making such a report.

Name

Job Title

Signature

Date

# Appendix 8: Transparency International Corruption Perception Index (<http://www.transparency.org/>)

| 2016 Rank | Country | 2016 Score | 2015 Score | Region |
| --- | --- | --- | --- | --- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | Denmark | 90 | 91 | Europe and Central Asia |
| 1 | New Zealand | 90 | 91 | Asia Pacific |
| 3 | Finland | 89 | 90 | Europe and Central Asia |
| 4 | Sweden | 88 | 89 | Europe and Central Asia |
| 5 | Switzerland | 86 | 86 | Europe and Central Asia |
| 6 | Norway | 85 | 88 | Europe and Central Asia |
| 7 | Singapore | 84 | 85 | Asia Pacific |
| 8 | Netherlands | 83 | 84 | Europe and Central Asia |
| 9 | Canada | 82 | 83 | Americas |
| 10 | Germany | 81 | 81 | Europe and Central Asia |
| 10 | Luxembourg | 81 | 85 | Europe and Central Asia |
| 10 | United Kingdom | 81 | 81 | Europe and Central Asia |
| 13 | Australia | 79 | 79 | Asia Pacific |
| 14 | Iceland | 78 | 79 | Europe and Central Asia |
| 15 | Belgium | 77 | 77 | Europe and Central Asia |
| 15 | Hong Kong | 77 | 75 | Asia Pacific |
| 17 | Austria | 75 | 76 | Europe and Central Asia |
| 18 | United States | 74 | 76 | Americas |
| 19 | Ireland | 73 | 75 | Europe and Central Asia |
| 20 | Japan | 72 | 75 | Asia Pacific |
| 21 | Uruguay | 71 | 74 | Americas |
| 22 | Estonia | 70 | 70 | Europe and Central Asia |
| 23 | France | 69 | 70 | Europe and Central Asia |
| 24 | Bahamas | 66 | N/A | Americas |
| 24 | Chile | 66 | 70 | Americas |
| 24 | United Arab Emirates | 66 | 70 | Middle East and North Africa |
| 27 | Bhutan | 65 | 65 | Asia Pacific |
| 28 | Israel | 64 | 61 | Middle East and North Africa |
| 29 | Poland | 62 | 63 | Europe and Central Asia |
| 29 | Portugal | 62 | 64 | Europe and Central Asia |
| 31 | Barbados | 61 | N/A | Americas |
| 31 | Qatar | 61 | 71 | Middle East and North Africa |
| 31 | Slovenia | 61 | 60 | Europe and Central Asia |
| 31 | Taiwan | 61 | 62 | Asia Pacific |
| 35 | Botswana | 60 | 63 | Sub Saharan Africa |
| 35 | Saint Lucia | 60 | N/A | Americas |
| 35 | Saint Vincent and the Grenadines | 60 | N/A | Americas |
| 38 | Cape Verde | 59 | 55 | Sub Saharan Africa |
| 38 | Dominica | 59 | N/A | Americas |
| 38 | Lithuania | 59 | 59 | Europe and Central Asia |
| 41 | Brunei | 58 | N/A | Asia Pacific |
| 41 | Costa Rica | 58 | 55 | Americas |
| 41 | Spain | 58 | 58 | Europe and Central Asia |
| 44 | Georgia | 57 | 52 | Europe and Central Asia |
| 44 | Latvia | 57 | 56 | Europe and Central Asia |
| 46 | Grenada | 56 | N/A | Americas |
| 47 | Cyprus | 55 | 61 | Europe and Central Asia |
| 47 | Czech Republic | 55 | 56 | Europe and Central Asia |
| 47 | Malta | 55 | 60 | Europe and Central Asia |
| 50 | Mauritius | 54 | 53 | Sub Saharan Africa |
| 50 | Rwanda | 54 | 54 | Sub Saharan Africa |
| 52 | Korea (South) | 53 | 54 | Asia Pacific |
| 53 | Namibia | 52 | 53 | Sub Saharan Africa |
| 54 | Slovakia | 51 | 51 | Europe and Central Asia |
| 55 | Croatia | 49 | 51 | Europe and Central Asia |
| 55 | Malaysia | 49 | 50 | Asia Pacific |
| 57 | Hungary | 48 | 51 | Europe and Central Asia |
| 57 | Jordan | 48 | 53 | Middle East and North Africa |
| 57 | Romania | 48 | 46 | Europe and Central Asia |
| 60 | Cuba | 47 | 47 | Americas |
| 60 | Italy | 47 | 44 | Europe and Central Asia |
| 62 | Sao Tome and Principe | 46 | 42 | Sub Saharan Africa |
| 62 | Saudi Arabia | 46 | 52 | Middle East and North Africa |
| 64 | Montenegro | 45 | 44 | Europe and Central Asia |
| 64 | Oman | 45 | 45 | Middle East and North Africa |
| 64 | Senegal | 45 | 44 | Sub Saharan Africa |
| 64 | South Africa | 45 | 44 | Sub Saharan Africa |
| 64 | Suriname | 45 | 36 | Americas |
| 69 | Greece | 44 | 46 | Europe and Central Asia |
| 70 | Bahrain | 43 | 51 | Middle East and North Africa |
| 70 | Ghana | 43 | 47 | Sub Saharan Africa |
| 72 | Burkina Faso | 42 | 38 | Sub Saharan Africa |
| 72 | Serbia | 42 | 40 | Europe and Central Asia |
| 72 | Solomon Islands | 42 | N/A | Asia Pacific |
| 75 | Bulgaria | 41 | 41 | Europe and Central Asia |
| 75 | Kuwait | 41 | 49 | Middle East and North Africa |
| 75 | Tunisia | 41 | 38 | Middle East and North Africa |
| 75 | Turkey | 41 | 42 | Europe and Central Asia |
| 79 | Belarus | 40 | 32 | Europe and Central Asia |
| 79 | Brazil | 40 | 38 | Americas |
| 79 | China | 40 | 37 | Asia Pacific |
| 79 | India | 40 | 38 | Asia Pacific |
| 83 | Albania | 39 | 36 | Europe and Central Asia |
| 83 | Bosnia and Herzegovina | 39 | 38 | Europe and Central Asia |
| 83 | Jamaica | 39 | 41 | Americas |
| 83 | Lesotho | 39 | 44 | Sub Saharan Africa |
| 87 | Mongolia | 38 | 39 | Asia Pacific |
| 87 | Panama | 38 | 39 | Americas |
| 87 | Zambia | 38 | 38 | Sub Saharan Africa |
| 90 | Colombia | 37 | 37 | Americas |
| 90 | Indonesia | 37 | 36 | Asia Pacific |
| 90 | Liberia | 37 | 37 | Sub Saharan Africa |
| 90 | Morocco | 37 | 36 | Middle East and North Africa |
| 90 | The FYR of Macedonia | 37 | 42 | Europe and Central Asia |
| 95 | Argentina | 36 | 32 | Americas |
| 95 | Benin | 36 | 37 | Sub Saharan Africa |
| 95 | El Salvador | 36 | 39 | Americas |
| 95 | Kosovo | 36 | 33 | Europe and Central Asia |
| 95 | Maldives | 36 | N/A | Asia Pacific |
| 95 | Sri Lanka | 36 | 37 | Asia Pacific |
| 101 | Gabon | 35 | 34 | Sub Saharan Africa |
| 101 | Niger | 35 | 34 | Sub Saharan Africa |
| 101 | Peru | 35 | 36 | Americas |
| 101 | Philippines | 35 | 35 | Asia Pacific |
| 101 | Thailand | 35 | 38 | Asia Pacific |
| 101 | Timor-Leste | 35 | 28 | Asia Pacific |
| 101 | Trinidad and Tobago | 35 | 39 | Americas |
| 108 | Algeria | 34 | 36 | Middle East and North Africa |
| 108 | Côte d´Ivoire | 34 | 32 | Sub Saharan Africa |
| 108 | Egypt | 34 | 36 | Middle East and North Africa |
| 108 | Ethiopia | 34 | 33 | Sub Saharan Africa |
| 108 | Guyana | 34 | 29 | Americas |
| 113 | Armenia | 33 | 35 | Europe and Central Asia |
| 113 | Bolivia | 33 | 34 | Americas |
| 113 | Vietnam | 33 | 31 | Asia Pacific |
| 116 | Mali | 32 | 35 | Sub Saharan Africa |
| 116 | Pakistan | 32 | 30 | Asia Pacific |
| 116 | Tanzania | 32 | 30 | Sub Saharan Africa |
| 116 | Togo | 32 | 32 | Sub Saharan Africa |
| 120 | Dominican Republic | 31 | 33 | Americas |
| 120 | Ecuador | 31 | 32 | Americas |
| 120 | Malawi | 31 | 31 | Sub Saharan Africa |
| 123 | Azerbaijan | 30 | 29 | Europe and Central Asia |
| 123 | Djibouti | 30 | 34 | Sub Saharan Africa |
| 123 | Honduras | 30 | 31 | Americas |
| 123 | Laos | 30 | 25 | Asia Pacific |
| 123 | Mexico | 30 | 31 | Americas |
| 123 | Moldova | 30 | 33 | Europe and Central Asia |
| 123 | Paraguay | 30 | 27 | Americas |
| 123 | Sierra Leone | 30 | 29 | Sub Saharan Africa |
| 131 | Iran | 29 | 27 | Middle East and North Africa |
| 131 | Kazakhstan | 29 | 28 | Europe and Central Asia |
| 131 | Nepal | 29 | 27 | Asia Pacific |
| 131 | Russia | 29 | 29 | Europe and Central Asia |
| 131 | Ukraine | 29 | 27 | Europe and Central Asia |
| 136 | Guatemala | 28 | 28 | Americas |
| 136 | Kyrgyzstan | 28 | 28 | Europe and Central Asia |
| 136 | Lebanon | 28 | 28 | Middle East and North Africa |
| 136 | Myanmar | 28 | 22 | Asia Pacific |
| 136 | Nigeria | 28 | 26 | Sub Saharan Africa |
| 136 | Papua New Guinea | 28 | 25 | Asia Pacific |
| 142 | Guinea | 27 | 25 | Sub Saharan Africa |
| 142 | Mauritania | 27 | 31 | Middle East and North Africa |
| 142 | Mozambique | 27 | 31 | Sub Saharan Africa |
| 145 | Bangladesh | 26 | 25 | Asia Pacific |
| 145 | Cameroon | 26 | 27 | Sub Saharan Africa |
| 145 | Gambia | 26 | 28 | Sub Saharan Africa |
| 145 | Kenya | 26 | 25 | Sub Saharan Africa |
| 145 | Madagascar | 26 | 28 | Sub Saharan Africa |
| 145 | Nicaragua | 26 | 27 | Americas |
| 151 | Tajikistan | 25 | 26 | Europe and Central Asia |
| 151 | Uganda | 25 | 25 | Sub Saharan Africa |
| 153 | Comoros | 24 | 26 | Sub Saharan Africa |
| 154 | Turkmenistan | 22 | 18 | Europe and Central Asia |
| 154 | Zimbabwe | 22 | 21 | Sub Saharan Africa |
| 156 | Cambodia | 21 | 21 | Asia Pacific |
| 156 | Democratic Republic of Congo | 21 | 22 | Sub Saharan Africa |
| 156 | Uzbekistan | 21 | 19 | Europe and Central Asia |
| 159 | Burundi | 20 | 21 | Sub Saharan Africa |
| 159 | Central African Republic | 20 | 24 | Sub Saharan Africa |
| 159 | Chad | 20 | 22 | Sub Saharan Africa |
| 159 | Haiti | 20 | 17 | Americas |
| 159 | Republic of Congo | 20 | 23 | Sub Saharan Africa |
| 164 | Angola | 18 | 15 | Sub Saharan Africa |
| 164 | Eritrea | 18 | 18 | Sub Saharan Africa |
| 166 | Iraq | 17 | 16 | Middle East and North Africa |
| 166 | Venezuela | 17 | 17 | Americas |
| 168 | Guinea-Bissau | 16 | 17 | Sub Saharan Africa |
| 169 | Afghanistan | 15 | 11 | Asia Pacific |
| 170 | Libya | 14 | 16 | Middle East and North Africa |
| 170 | Sudan | 14 | 12 | Middle East and North Africa |
| 170 | Yemen | 14 | 18 | Middle East and North Africa |
| 173 | Syria | 13 | 18 | Middle East and North Africa |
| 174 | Korea (North) | 12 | 8 | Asia Pacific |
| 175 | South Sudan | 11 | 15 | Sub Saharan Africa |
| 176 | Somalia | 10 | 8 | Sub Saharan Africa |

# Appendix 9: PEP Questionnaire: Identification of Politically Exposed Persons (PEP’s)

According to the 3RD & 4th EU-Directive, Credit or Financial Institutions must gather sufficient information to determine whether a natural person is a Politically Exposed Person.

**Are you or have you been (during the past 18mths) entrusted with a Prominent public function?1**

If yes, please provide us with;

Description and role of the public function: …………………………………………………………………………………………….

…………………………………………………………………………………………………………………………………………………

Start date function : …….../………/…………..

End date function : ……../………/…………..

**Are you related (in terms of immediate family member2 or Close asscoiate3 to a natural person who is or has been (during the past year) entrusted with a Prominent Public function?**

If yes, please provide us with the exact title of the public function as well as the identity and your relationship with the involved natural person(s)

Surname, first name ………………………………………………………………………………..

Relationship: ……………………………………………………………………………………………………………………..

Description and role of the public function: ……………………………………………………………………………………

………………………………………………………………………………………………………………………………………

Start date function: ……../……../…………

End date function: ……../……../…………

I agree to inform your institution immediately in event this situation might change in a future date.

Signature: ……………………………………………………………….

1 Heads of state, heads of government, ministers and deputy or assistant ministers; members of parliaments; members of supreme courts, of constitutional courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances; members of courts or auditors or of the boards of central banks; ambassadors, charges d’affaires and high ranking officers in the armed forces; members of the administrative, management or supervisory bodies of State-owned enterprises; these categories do not include middle ranking or more junior officials.

2 The spouse, any partner considered by national law as equivalent to the spouse, the children and their spouses or partners and the parents.

3- Any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relation, with a person who is or has been entrusted with a prominent public function.

Any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is or has been entrusted with a prominent public function.

# Appendix 10: Beneficial Owner Declaration

Under existing laws concerning money laundering and terrorist financing (Money Laundering Regulations 2017, Bribery Act 2010, Financial Services and Markets Act 2000, European Commission Third Money Laundering Directive 2005 and Fourth Directive 2014) we are required to identify the Beneficial Owners for whose account our customers carry out transactions. Beneficial Owners mean the natural person(s) who ultimately owns or controls the Customer and/or the natural person, or listed institution, on whose behalf a transaction or activity is being conducted.

The undersigned 1

|  |  |  |  |
| --- | --- | --- | --- |
| Surname and first name | Capacity 2 | Signature(s) |  |
| A) |  | A) | B) |
| B) |  |
| C) |  | C) | D) |
| D) |  |

Acting as Legal Representative(s) for;

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Customer | Postcode | Town/City and country of registered office | Company number |
|  |  |  |  |

Declare(s), that on ……../……../20….. (date), the Beneficial Owner of the Customer are the following **natural persons** holding 10% or more of the company shares/voting rights:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Surname and first name/s 1 | Date of birth | Place of birth | Home address ( street, number ,town/city, country) | Occupation | No. of Identification document | Capacity of Beneficial Owner 3  & % of shares owned. |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

…or that the **Beneficial Owner** is the following **exchange listed company**:

|  |  |  |
| --- | --- | --- |
| Company name | Address of Registered Office | Stock exchange on which company is listed |
|  |  |  |

The customer undertakes irrevocably to notify the bank, in writing and without delay, of any change made to the Beneficial Owners detailed in this list and to provide the bank with a copy of the identification documents of the new Beneficial Owners. The bank reserves the right to terminate, without having to provide compensation or advance notice, any and all relations with the customer if it transpires that the bank was notified of the above mentioned change. The bank will notify the customer of any such termination of relations by ordinary letter.

1. If not already supplied, attach a copy of the back and front of the identity card/ passport. If the identification document does not show an address, attach a copy of another official document that does contain the address.
2. State the job title of the persons authorised to represent the legal entity (e.g. director, chairman, managing director).
3. State the capacity of the Beneficial Owner (e.g. shareholder, director…)

# Appendix 11 Useful Links

**National Crime Agency (NCA)**

[www.NCA.gov.uk](http://www.soca.gov.uk)

**NCA Disclosure Form**

NCA has prepared a standard disclosure form. Both this form and guidance on completing it are available at [www.NCA.gov.uk/financialIntel/disclosure.html#forms](http://www.soca.gov.uk/financialIntel/disclosure.html#forms).. NCA prefers reports to be delivered electronically and the details of how to register can be found at <https://www.ukciu.gov.uk/saronline.aspx>.

**List of Regulators**

<http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=773&menu=expand>

**Home Office Proscribed Organisations List**

<http://www.homeoffice.gov.uk/security/terrorism-and-the-law/terrorism-act/proscribed-groups?version=1>

**HM Treasury Sanctions List**

<http://www.hm-treasury.gov.uk/documents/financial_services/sanctions/fin_sanctions_index.cfm>

**Worldwide Registries (Companies House equivalents)** <http://www.companieshouse.gov.uk/links/introduction.shtml>

**Professional Bodies**

<http://www.companieshouse.gov.uk/links/introduction.shtml>

**Comparable Jurisdictions**

Comparable jurisdictions can be summarised as the following:

* EU Member States including Gibraltar as part of the UK, and Netherlands Antilles and Aruba as part of the Kingdom of the Netherlands,
* EEA Countries
* UK Crown Dependencies
* Non-UK FATF Members

It does not exempt {XYZ LIMITED} from performing wider due diligence and Know Your Customer checks. Neither the “comparability” status provides an exemption from the objective test in the Proceeds of Crime Act 2002. “Comparability” indicates that client identification procedures exist in a country. This is based on the provisions of the legislation in a particular jurisdiction, rather than what actually happens in practice. This applies to both EU Member States and non-EU countries which are "comparable jurisdictions".

<http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=770&a=9814>

**Financial Action Task Force**

The inter-governmental body known as the ‘Financial Action Task Force’ (“FAFT”)’ was established to develop and promote policies, both at national and international levels on combating money laundering and terrorist financing. FATF member countries have committed themselves to implementing the FATF Forty Recommendations which in several respects are more wide-ranging in nature than the provisions of the European Money Laundering Directives. Membership of this inter-governmental body is subject to ongoing approval and monitoring.

[www.fatf-gafi.org](http://www.fatf-gafi.org)

**FATF Member Countries**

<http://www.fatf-gafi.org/document/52/0,3343,en_32250379_32237295_34027188_1_1_1_1,00.html>

Recognised Investment Exchanges, Recognised Overseas Investment Exchanges, Recognised Clearing Houses, Recognised Overseas Clearing Houses, Designated Investment Exchanges and Regulated Markets

[http://www.FCA.gov.uk/register/exchanges.do](http://www.fsa.gov.uk/register/exchanges.do)

https://register.fca.org.uk/shpo\_searchresultspage?preDefined=ROIE&TOKEN=3wq1nht7eg7tr

**Sanctions**

Office of Financial Sanctions Implementation (OFSI) is part of HM Treasury and helps to ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom. <https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation>

**Panama Papers Database**

<https://offshoreleaks.icij.org/>

1. An Introduction Certificate is a Certificate that states that one regulated entity has conducted appropriate checks to satisfy money laundering requirements for a client. This certificate can be forwarded to another regulated entity and can be relied upon to satisfy money laundering requirements by the entity receiving the Certficate. [↑](#footnote-ref-1)