

Anti-Money Laundering Policy

Version: 1.0 (March 2025)

WWW.NOORCAPITAL.CO.UK

Noor Capital UK Limited is authorized and regulated by the Financial Conduct Authority. UK FCA Register Number: 631382.
Registered in England and Wales, number: 09137156.

Version Control

Document Owner: *Suhail Bajwa*

Version No:	Date:	Version Author:	Approved By:	Approval Date:	Revisions/Changes:
1.0	20/01/2025	<i>Suhail Bajwa</i>	<i>Board</i>	24/01/2025	

Contents

1	Purpose	5
2	Review of Policy	5
3	Responsibilities.....	5
4	Definition of Money Laundering and Terrorist Financing	5
4.1	Key stages of money laundering.....	5
4.2	Money Laundering and Terrorist Financing Offences.....	6
4.2.1	Failure to disclose	6
4.2.2	Tipping Off.....	6
4.3	Consequences of non-compliance	6
5	Risk management and Controls	7
5.1	Client Due Diligence.....	7
5.1.1	Private individuals.....	9
5.1.1.1	Identifying private individuals as clients	9
5.1.1.2	Verifying identities of private individuals.....	9
5.1.2	Corporate clients.....	10
5.1.2.1	Identifying corporate clients	10
5.1.2.2	Verifying identities of corporate clients	10
5.1.3	Unincorporated clients	11
5.1.3.1	Identifying unincorporated clients	11
5.1.3.2	Verifying identities of unincorporated clients.....	11
5.1.4	Public sector body, government, state owned company and supranational clients	11
5.1.4.1	Identifying public sector body, government, state owned company and supranational clients	11
5.1.4.2	Verifying identities of public sector body, government, state owned company and supranational clients	11
5.1.5	Pension scheme clients.....	11
5.1.6	Cryptoasset Exchange Providers (CEP).....	11
5.1.7	Charity, church body, trust and foundation clients	12
5.1.7.1	Identifying charity, church body, trust and foundation clients	12
5.1.7.2	Verifying identities of charity, church body, trust and foundation clients.....	12
5.1.8	Politically Exposed Persons (PEP).....	12
5.1.9	Nature of Business	14
5.1.10	Shell Banks	14
5.2	Customer Risk Assessment	
5.3	Enhanced Due Diligence (EDD).....	14
5.4	Financial Sanctions	15
5.5	Ongoing Monitoring	17
5.5.1	Red Flags	17
5.5.2	Transaction monitoring.....	18
5.5.3	Client reviews.....	19
5.5.3.1	Re-verification of identification.....	19

5.5.3.2	High Risk Clients	19
5.5.3.3	Medium Risk Clients	19
5.5.3.4	Low Risk Clients	20
5.5.3.5	Trigger events.....	20
5.5.1	Nominated Officer Reviews	20
5.6	<i>Reporting Suspicious Transactions</i>	20
5.6.1	Subsequent investigations	21
5.7	<i>Record Keeping</i>	21
6	Breaches of Anti-Money Laundering Policy	22
7	Annex 1 - Source of wealth and origin of funds information and evidential guide	23

1 Purpose

This policy details how Noor Capital UK Limited (the Firm) will manage the risks posed by money laundering and ensure a consistency of approach within the firm.

The Firm is authorised by the Financial Conduct Authority (FCA) and, as such, will act in accordance with the anti-money laundering rules as defined by the relevant statutory authorities.

The Firm's has a zero tolerance for money laundering and is committed to mitigating the risks of money laundering. The firm will take the necessary preventative actions and will promptly investigate any suspicion of money laundering occurring.

For the purpose of this policy, money laundering also includes any activities relating to terrorist financing.

This policy should be read in conjunction with the Financial Crime Policy.

2 Scope and applicability

Noor Capital UK Limited has a comprehensive approach to dealing with Financial Crimes risks including ML. Firm's Financial Crime Policy is designed with the objective to provide a consistent, coherent and proportionate approach to, deterring, detecting preventing and reporting all types of 'financial crime' across the firm.

3 Review of Policy

This policy will be reviewed regularly, at least once a year, and amended as considered necessary by the Firm's Management Body in the event of changing circumstances or regulations.

4 Responsibilities

The responsibilities of the Management Body, Nominated Officer and Employees are documented in the Firm's Financial Crime Policy.

This policy will be communicated to all staff during their induction to the Firm and any updates will be communicated via email from the MLRO/Nominated officer.

5 Definition of Money Laundering and Terrorist Financing

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of income. The risks to the financial sector primarily involve being used to facilitate this process, whether knowingly or unwittingly.

Terrorist Financing is all dealings with funds or property which are, or are likely to be, used for the purposes of terrorism, even if the funds are "clean" in origin.

For the purpose of this policy, money laundering also includes any activities relating to terrorist financing.

5.1 Key stages of money laundering

Money laundering is generally broken down into in three distinct stages:

- Placement– this is the first stage in the money laundering operation and involves the physical disposal of the initial proceeds derived from illegal activity, e.g. placing cash in the conventional financial system
- Layering– this second stage involves separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity
- Integration– the final stage involves providing an apparent legitimacy to the criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

5.2 Money Laundering and Terrorist Financing Offences

A money laundering offence may be committed if a person:

- Conceals, disguises or transfers criminal property
- Enters into or becomes involved in an arrangement which he knows or suspects facilitates the acquisition, retention, use or control of criminal property on behalf of another person
- Acquires, uses or has possession of criminal property

In the case of terrorism financing, an offence is committed if there is involvement in providing money, or other property, to be used for the purposes of terrorism, even if the funds are clean in origin.

5.2.1 Failure to disclose

Employees working for a regulated firm, such as the Firm, would commit an offence if they fail to make a disclosure to the authorities or in the form of an internal report to the Nominated Officer in cases where they have knowledge or suspicion that money laundering or terrorism financing is occurring.

5.2.2 Tipping Off

An offence of “Tipping off” is committed when anyone discloses to a person who is the subject of a suspicious report, or a third party, that a disclosure has been made to the Nominated Officer or the authorities or that an investigation is being carried out, as this could prejudice the investigation.

Making enquiries of a client, to verify identity or to ascertain the source of funds for a particular transaction will not trigger a tipping off offence before a suspicious activity report has been submitted in respect of that client. If a suspicious activity report has been made, great care should be taken to ensure the client does not become aware of that fact.

5.3 Consequences of non-compliance

Non-compliance with the money laundering obligations by employees is considered a serious offence and disciplinary actions may be taken by the Firm, including immediate dismissal.

Failure to comply with the money laundering obligations may also result in a criminal penalty (including imprisonment).

The penalties for those found guilty of assisting or failing to report money laundering are severe:

- Up to 14 years in prison, a fine, or both for knowingly assisting in money-laundering

- Up to 5 years in prison, a fine, or both for failing to report any knowledge or suspicions of money-laundering
- Up to 2 years in prison, a fine, or both for alerting a suspected money-launderer that a report has been made to the Nominated Officer or the authorities, or that the authorities are investigating or proposing to investigate

In addition to these criminal penalties, a breach of these rules could cause significant damage to the reputation of the Firm and its employees. Failure to comply by an employee may also expose the Firm to penalties, censure and enforcement action (including the impositions of fines) by the FCA or other regulatory body.

6 Risk management and Controls

Noor Capital UK Limited has a comprehensive Approach to dealing with Financial Crimes risks including ML. Firm's Financial Crime Policy is designed with the objective to provide a consistent, coherent and proportionate approach to, deterring, detecting preventing and reporting of all types of 'financial crime' across the firm.

6.1 Customer Risk Assessment

The Firm is required to adopt a risk-based approach to comply with its AML obligations. This is in order to enable focus of a control framework on those customers, products, channels and jurisdictions that are assessed as carry a greater Money Laundering or Terrorist Financing risk.

The Firm will assess the risk for each client taking into account the purpose of the account or relationship, the level of assets involved or the size of transactions to be undertaken and the regularity or duration of the business relationship.

The client risk assessment will also take into account customer risk factors (including nature of business), product, service, transaction or delivery channel risk factors and geographical risk factors.

Low Customer risk factors:

- a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership
- b) public administrations or enterprises
- c) customers that are resident in geographical areas of lower risk

High Risk Customer risk factors:

- a) the business relationship is conducted in unusual circumstances
- b) customers that are resident in geographical areas of higher risk
- c) legal persons or arrangements that are personal asset-holding vehicles
- d) companies that have nominee shareholders or shares in bearer form
- e) businesses that are cash-intensive
- f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business

Low Product, service, transaction or delivery channel risk factors:

- a) life insurance policies for which the premium is low
- b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral

- c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme
- d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes
- e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money)

High Product, service, transaction or delivery channel risk factors:

- a) private banking
- b) products or transactions that might favour anonymity
- c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures
- d) payment received from unknown or un-associated third parties
- e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products

Low Geographical risk factors:

- a) Member States
- b) third countries having effective Anti-Money Laundering systems
- c) third countries identified by credible sources as having a low level of corruption or other criminal activity
- d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing and effectively implement those requirements

High Geographical risk factors

- a) Countries listed on The Money Laundering and Terrorist Financing (Amendment) (High Risk Countries) Regulations 2021, the UK High Risk Third Country List
- b) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective Anti-Money Laundering systems
- c) countries identified by credible sources as having significant levels of corruption or other criminal activity
- d) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations
- e) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country

Clients will be classified into a risk category – high, medium or low risk. Clients that are identified with any high-risk factors will have to undergo Enhanced Due Diligence.

Where the Firm uses Agents to procure business on its behalf, it will ensure that these Agents perform adequate Due Diligence.

6.2 Client Due Diligence

The Firm's client due diligence consists of the following:

Identifying the client and verifying the client's identity using documents or information from a reliable and independent source

Identifying the beneficial owner(s) and verifying that person's identity, taking measures to understand the ownership and control structure of the client, where applicable

Assessing the purpose and intended nature of the business relationship (business profile)

Conducting ongoing monitoring of the business relationship and transactions undertaken to ensure that they are consistent with the Firm's knowledge of the client, business, risk profile and source of funds

The Firm will also ensure that anyone acting on behalf of the client is authorised to do so and will identify and verify the identity of that person.

The Firm will ensure that clients are identified and that their identity is verified before commencing any transactions with them.

The Firm uses the Refinitiv World Check to conduct checks relating to the following:

- PEPs
- Sanctions
- Electronic ID documents Verification

6.2.1 Private individuals

6.2.1.1 Identifying private individuals as clients

The Firm will obtain the following information for prospective clients that are individuals:

Full name

Residential address

Date of birth

6.2.1.2 Verifying identities of private individuals

The Firm will verify the information obtained using reliable and independent sources, either by viewing documentation from the client or via electronic checks.

Documentary evidence should include government issued documents with photos, such as valid passport, photo card driving licence or national identity card, or government issued documents without photos which incorporate the client's full name and either his residential address or his date of birth, supported by a second document either government issued, issued by a judicial authority, a public sector body, a regulated utility company or another FCA regulated firm in the UK.

Electronic verification will include the client's full name, address and date of birth and will be carried out by a provider who is registered with the Information Commissioner's Office, use a range of positive information sources, can access negative information sources and that has a transparent process.

When electronic verification is used or a client has not been physically present for identification purposes, the Firm will carry out an additional verification check to manage the risk of impersonation fraud. This check may take the form of:

Requiring the first payment to be carried out through an account in the client's name with a UK or EU regulated credit institution

Telephone contact with the client on a home or business number that has been verified, prior to opening the account

Communicating with the client at the address that has been verified

Requiring copy documents to be certified by an appropriate person

The Firm will consider on a case by case basis any clients that cannot reasonably be expected to produce the standard evidence of identity and will seek to agree the use of other confirmations of identity so that clients are not unreasonably denied access to the products and services.

Any exceptions to this policy will be recorded by the Nominated officer/MLRO and maintained in a register which is reviewed at least annually.

6.2.2 Corporate clients

6.2.2.1 Identifying corporate clients

The Firm will obtain the following information for prospective clients that are corporates:

Full name

Registered number

Registered office in country of incorporation

Business address

And for private or unlisted companies:

Names of all the directors

Names of individuals who own or control over 25% of its shares or voting rights

Names of any individuals who exercise control over the management of the company

Names of ALL beneficial owners (where practicable) for Sanctions and PEP screening

- The Firm will take reasonable steps to identify the beneficial ownership and controllers of the corporate. It will keep records of the actions taken to determine such.

6.2.2.2 Verifying identities of corporate clients

The Firm will verify the identity of the client by confirming the company's listing on a regulated market, searching the relevant company registry or viewing a copy of the company's Certificate of Incorporation. If there is a discrepancy between the company register and the client information, then the Firm will update the company register with the correct information. Refer to <https://www.gov.uk/guidance/report-a-discrepancy-about-a-beneficial-owner-on-the-psc-register-by-an-obliged-entity> for further guidance.

The Firm will also ensure that anyone acting on behalf of the client is authorised to do so and will identify and verify the identity of that person.

The Firm will ensure that at least one director is identified and verified.

6.2.3 Unincorporated clients

6.2.3.1 Identifying unincorporated clients

The Firm will obtain the following information for prospective clients that are unincorporated:

Full name

Business address

Names of all the partners/principals who exercise control over the management of the business

Names of individuals who own or control over 25% of its capital/profit or voting rights

6.2.3.2 Verifying identities of unincorporated clients

The Firm will verify the identity of the client by using information from an independent and reliable source, confirming the client's membership of a relevant professional or trade association, viewing the partnership deed or treating the client as a collection of private individuals.

The Firm will also ensure that anyone acting on behalf of the client is authorised to do so.

6.2.4 Public sector body, government, state owned company and supranational clients

6.2.4.1 Identifying public sector body, government, state owned company and supranational clients

The Firm will obtain the following information for prospective clients that are public sector bodies, governments, state owned companies or supra-nationals:

Full name of entity

Nature and status of entity

Address of the entity

Name of the home state authority

Names of directors

6.2.4.2 Verifying identities of public sector body, government, state owned company and supranational clients

The Firm will ensure that anyone acting on behalf of the client is authorised to do so and will identify and verify the identity of that person.

6.2.5 Pension scheme clients

The Firm will check the HMRC register or Pensions Regulator for evidence of registration which will be sufficient to meet the identification and verification requirements.

6.2.6 Cryptoasset Exchange Providers (CEP)

The Firm will obtain the following information for prospective clients that are CEP's:

Full name

Registered number

Registered office in country of incorporation

Business address

Name of regulator and registration number

And for private or unlisted companies:

Names of all the directors

Names of individuals who own or control over 25% of its shares or voting rights

Names of any individuals who exercise control over the management of the company

Names of ALL beneficial owners (where practicable) for Sanctions and PEP screening

The Firm will take reasonable steps to identify the beneficial ownership and controllers of the corporate. It will keep records of the actions taken to determine such.

6.2.7 Charity, church body, trust and foundation clients

6.2.7.1 Identifying charity, church body, trust and foundation clients

The Firm will obtain the following information for prospective clients that are charities, church bodies, trusts or foundations:

Full name and address

Nature of activities and objects

Names of all trustees

Names or classes of beneficiaries

Country of establishment (for trusts and foundations)

Name and address of any protector or controller (for trusts and foundations)

6.2.7.2 Verifying identities of charity, church body, trust and foundation clients

The Firm will verify the identity of the client by using information from an independent and reliable source, the Charity Commission, Office of the Scottish Charity Regulator, HMRC's confirmation of church's application for charitable status, through headquarters of the religion, sight of trust deeds or register in country of establishment.

The Firm will also verify the identities of the trustees.

6.2.8 Politically Exposed Persons (PEP)

A PEP is defined as "an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person". This definition applies to those holding such a position in a state inside or outside the UK, or in a community institution or an international body.

A PEP may also be:

- direct customer dealing with the Firm on his/her own behalf
- Person linked to , or associated with an entity or non-personal account (e.g. a key account party to a corporate account)(Note: the entity or corporate is not a PEP)

For the purposes of this policy that all PEPs must be identified regardless of the jurisdiction in which they hold, or held office in the preceding year.

PEPs can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities, however, it does put the client, or the beneficial owner, into a higher risk category.

Where the Firm specifically deals with PEPs of the USA, it will comply with the provision of the Foreign and Corrupt Practices Act (1977) (FCPA).

The Firm will check all clients at initial account set up and at least quarterly to identify any PEPs, using World Check or another source. If a PEP is identified, the Nominated Officer will be notified and enhanced due diligence measures will be employed.

Factors that will be considered in assessing the level of risk posed by the PEP include but are not limited to:

- Geographic location
- Official responsibilities of the individual and their office
- Nature of their title (i.e. whether it is honorary or salaried)
- Level and nature of authority or influence over government activities or other officials
- Access to significant government assets or funds
- Source of wealth and source of funds to be used for the transaction

Once due diligence is complete, approval will be sought from the Nominated Officer prior to completion of account set up or any transactions being carried out. The Nominated officer must ensure these procedures are in place to identify, document and assess ML risk posed by PEPs and PEP associates.

Where approval is granted to continue with the PEP relationship the reasoning will be documented by the Nominated Officer and the nature and extent of the on-going monitoring of the account will be agreed with the relevant teams in the Firm. The name of the PEP will be added to the Firm's PEP register.

Where approval is not granted to continue with the PEP relationship, the Nominated Officer, in liaison with the relevant teams, will ensure that the any identifiable money laundering risk is assessed and dealt with appropriately, the client relationship is exited and that the client is treated fairly.

The Firm will maintain a register of PEPs which will be regularly reviewed (at least annually) by the Nominated Officer.

Enhanced Due Diligence must be conducted on all PEPs. EDD applied to PEPs must demonstrates clear difference from CDD/SDD measures.

6.2.9 Nature of Business

The Firm will obtain and record sufficient information on the client's nature of business and the purpose of the account, including expected source of funds, source of wealth and anticipated transaction volumes and values. This will enable an assessment of whether the purpose of the account to be opened is consistent with the nature of business.

6.2.10 Shell Banks

The Firm will not deal with Shell Bank or corporations. The Firm will verify the physical address of the bank and their banking or corporate registration details.

In addition the firm will not:

- enter into , or continue to have a relationship with another firm which is known to permit its accounts to be used by a shell bank.
- set up an anonymous account of any sort for a new or existing customer,

6.3 Enhanced Due Diligence (EDD)

Enhance Due Diligence is performed by The Firm when clients are identified with any high-risk factors for financial crime, however the extent of the enhanced due diligence will depend on the reason why a relationship with the client is classed as high risk. The Firm will take an informed decision, agreed with the Nominated Officer, about which enhanced due diligence measures are appropriate in each high-risk situation.

The Firm's enhance due diligence measures include:

Increasing the quantity of information obtained for client due diligence purposes:

- i. About the client's or beneficial owner's identity, or ownership and control structure, to be satisfied that the risk associated with the relationship is well known. This may include obtaining and assessing information about the client's or beneficial owner's reputation and assessing any negative allegations against the client or beneficial owner. Examples include: information about family members and close business partners; information about the client's or beneficial owner's past and present business activities; and adverse media searches
- ii. About the intended nature of the business relationship, to ascertain that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete client risk profile. It includes obtaining information on:
- iii. the number, size, frequency and reason for the transactions that are likely to pass through the account to be able to spot deviations that may give rise to suspicions, requesting evidence where appropriate
- iv. the reason the client is looking for a specific product or service, in particular where it is unclear why the client's needs cannot be met better in another way, or in a different jurisdiction
- v. the destination of funds
- vi. the nature of the client's or beneficial owner's business to understand the likely nature of the business relationship better

Increasing the quality of information obtained for client due diligence purposes to confirm the client's or beneficial owner's identity including by:

- i. Requiring the first payment to be carried out through an account verifiably in the client's name with a bank subject to UK Client Due Diligence standards
- ii. Establishing that the client's source of wealth and source of funds that are used in the business relationship are not the proceeds from criminal activity and that they are consistent with The Firm's knowledge of the client and the nature of the business relationship. The sources of funds or wealth may be verified, among others, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent and credible media reports

Increasing the frequency of reviews, to be satisfied that The Firm continues to be able to manage the risk associated with the individual business relationship and to help identify any transactions that require further review, including by:

Obtaining the approval of the MLRO/nominated officer to commence or continue the business relationship to ensure senior management are aware of the risk The Firm is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk

Reviewing the business relationship on a more regular basis to ensure any changes to the client's risk profile are identified, assessed and, where necessary, acted upon , on-going monitoring and review context and frequency of which should be agreed with the Nominated Officer. The Nominated Officer

Conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that may give rise to suspicion of money laundering or terrorist financing. This may include establishing the destination of funds or ascertaining the reason for certain transactions

The Nominated Officer will need to provide approval, or refusal, to proceed with the client set up process prior to conducting any business with a client who has been through the enhanced due diligence process

The Management Body will consider its risk appetite in relation to clients. The Nominated Officer may decide to reject existing or new clients on the basis of Financial Crime concerns. The Management Body will be informed and the relevant client closing procedure will be followed.

6.4 Simplified Due Diligence (SDD)

The Firm may apply SDD measures in relation to a particular business relationship or transaction if it determines that, taking into account its risk assessment, the business relationship or transaction presents a low degree of risk of ML/TF.

When assessing whether there is a low degree of risk of ML/TF in a particular situation, and the extent to which it is appropriate to apply SDD measures in that situation.

The firm must take account of at least the following risk factors before deciding whether it is appropriate to apply SDD:

Whether the customer is:

- a public administration, or a publicly owned enterprise

- an individual resident in a geographical area of low risk
- a credit or financial institution subject to the requirements in the fourth and fifth money laundering directive
- a company listed on a regulated market

A determination that SDD measures may be applied in a particular situation does not remove the obligation to conduct ongoing monitoring of the business relationship, although the extent of this may be adjusted to reflect its determination of the low degree of ML/TF risk. Such determination does not affect the duty to report knowledge or suspicion of money laundering or terrorist financing.

In the event the risk assessment identifies higher risk factors (e.g. High risk country, PEPs, complex structures etc.) SDD cannot be applied and EDD must be applied instead.

Also, if it is identified that the customer through its daily activities

- Reaches a certain threshold
- where the firm had come into possession of news or information that brings doubt to the accuracy of the current CDD information held
- when the Firm has identified activity deemed to be suspicious

EDD must be applied in line with section 5.3 above.

The Firm should also document the rationale for the decision to apply SDD and this must be signed off by the MLRO

6.5 Financial Sanctions

The Firm will review all clients to ensure that they are not on the Financial Sanctions register as published by HM Treasury or other relevant body (e.g. UN, EU and OFAC Sanction Lists, at initial client set up and then periodically on a risk based approach. The Firm will not set up accounts for clients on the Financial Sanctions Register or carry out any transactions with them. The Firm will screen all incoming and outgoing transaction beneficiaries for Sanctioned status.

It is a criminal offence to make funds or financial services available to individuals or entities on the sanctions list without a licence. The latest list can be found here:

<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>

The Firm will complete checks on clients to ensure that they are not on the financial sanctions register before proceeding with the account set up.

Employees will discuss any clients that appear on the sanctions list with the Nominated Officer in the first instance. If a prospective client is on the sanctions list and the Firm does not hold a relevant licence to proceed, then the Firm will halt further account set up and report the matter to the Office of Financial Sanctions at the HM Treasury – contact details as follows:

Office of Financial Sanctions Implementation
HM Treasury
1 Horse Guards Road
London SW1A 2HQ

TEL. 020 7270 5454 or email ofsi@hmtreasury.gsi.gov.uk

The Firm has subscribed to email updates of the sanctions list on the HM Treasury website (<https://public.govdelivery.com/accounts/UKHMTREAS/subscriber/new>) to keep up to date with any changes. New additions to the list will be checked against the Firm's existing client lists and any positive matches will be reported to the Office of Financial Sanctions at the HM Treasury immediately and any funds or transactions will be frozen.

The Firm will continually and no less than a monthly basis, monitor the client lists against the sanctions list and any positive matches will be reported to the Office of Financial Sanctions at the HM Treasury immediately.

6.6 Ongoing Monitoring

The Firm will take a risk based approach in continually monitor its clients for signs of money laundering, focusing on transaction monitoring and client reviews. The Firm will perform this by applying a differing levels of monitoring based on the risk rating of the client.

6.6.1 Red Flags

Red flags are client behaviours or issues with client's business that should act as a warning that further investigation by the Firm is necessary. Red flags can be identified during on-going monitoring i.e. CDD review and transaction monitoring.

Examples of red flags are:

- Client is reluctant to provide information or is evasive
- Client's lifestyle appears in excess of known sources of income
- Client's business structure is unnecessarily complicated
- Involvement of third parties without valid reason
- Unusual instructions
- Repeated or inexplicable changes to instructions
- Use of bank accounts without valid reason
- Complex structuring of transactions without valid reason
- Client's disinterest in prices, commissions, costs etc.
- Transactions out of line with expected transaction for the client
- Unexplained transfers of funds
- 3rd parties making unexpected repayments for a customer
- Repayments from multiple bank accounts held by a customer

Transactions are inconsistent with business activities of customer

Purpose of customer account changes without adequate explanation or oversight

Transactions unexpectedly involve high risk jurisdictions, sectors or individuals

Early repayment of loans or increased size/ frequency of repayments

Accounts with low balances but a high volume of large debits and credits

Cumulative turnover significantly exceeds the customer's expected income / expected activity

Debits are made shortly after credits for the same value are received

Customer makes frequent transactions just below the transaction monitoring alert thresholds

Debits to and credits from 3rd parties with no obvious explanation for the transaction

Customer provides insufficient or misleading information about a transaction or is evasive

If any red flags are identified in the Client Due Diligence or monitoring processes, employees must notify the Nominated Officer immediately.

6.6.2 Transaction monitoring

The Firm will continuously monitor client's transactions to detect unusual transactions or patterns of transactions and to ensure that any unusual or suspicious activity is identified and investigated immediately.

Based on the Firm's knowledge of the client, the monitoring will look for:

- Unusual behaviour - sudden and/or significant changes in transaction activity by value, volume or nature, such as change in beneficiary or destination
- Linked relationships – identifying common beneficiaries and remitters amongst apparently unconnected accounts or clients
- High risk geographies and entities - significant increases of activity or consistently high levels of activity with higher risk geographies and/or entities
- Other money laundering behaviours – indications of possible money laundering, such as the structuring of transactions under reporting thresholds, transactions in round amounts, overly complex transactions
- Dormant relationships

The Firm will carry out retrospective reviews on the client to ensure the business being transacted is consistent with what was anticipated when the client was taken. The frequency will depend on the risk classification of the client:

- High Risk will be reviewed no less than weekly
- Medium Risk will be reviewed no less than monthly
- Low Risk will be reviewed on a real-time risk basis and may not need to undergo a retrospective check

Where unusual patterns are identified, then enhanced due diligence will be carried out. Enhanced due diligence will include:

- Establishing the source and destination of the funds

- Finding out more about the client's business to understand the rationale and reason for the transactions
- Monitoring the business relationship and subsequent transactions more frequently

Any suspicious activity will be reported to the Nominated Officer for further investigation or reporting to the necessary authorities.

The Firm uses a combination of manual and automated transaction monitoring. The Firm determines appropriate thresholds in accordance with the risk rating of the client in conjunction with the Business Wide Risk assessment.

The firm Rationale for determining appropriate transaction monitoring (manual or automated) must be documented and approved by the Nominated Officer and Board Audit Risk Compliance Committee (ARCC).

6.6.3 Client reviews

The Firm will ensure that client due diligence information is relevant and kept up to date via regular client reviews. The extent to which client reviews are undertaken will be determined using a risk-based approach and applied in accordance with the risk rating applied to the client during the client risk assessment.

The Firm has a customer review process based on the High, Medium and Low risk factors assigned to its clients.

6.6.3.1 Re-verification of identification

Once the identity of a client is satisfactorily verified, there will usually be no need to re-verify identity, unless the client name changes, the beneficial ownership or control changes materially, subsequent doubts arise as to the accuracy of evidence previously obtained or a new risk emerges.

6.6.3.2 High Risk Clients

On an annual basis, all clients, who have been classed as high risk, will undergo a complete review. This will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Corporate Structure (if applicable)
- Re-confirmation of nature of the business relationship (if applicable)
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse news, PEP and Sanctions
- Complete review of transaction profile, including new products requested

6.6.3.3 Medium Risk Clients

Medium Risk customers will undergo a full review every two years. This will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Corporate Structure (if applicable)
- Re-confirmation of nature of the business relationship (if applicable)
- Screening for adverse news, PEP and Sanctions

- Complete review of transaction profile, including new products requested

The information obtained during the review will be assessed to determine if the medium risk rating still applies.

6.6.3.4 Low Risk Clients

Low risk customers will be reviewed every 3 years or when trigger events occur such as:

- the customer looking to take out a new product or service, or when a certain transaction threshold is reached
- where the firm had come into possession of news or information that brings doubt to the accuracy of the current CDD information held
- when the Firm has identified activity deemed to be suspicious

This review will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Corporate Structure (if applicable)
- Re-confirmation of nature of the business relationship (if applicable)
- Screening for adverse news, PEP and Sanctions
- Complete review of transaction profile, including new products requested

The information obtained during the renewal will be assessed to determine if the low risk rating still applies.

6.6.3.5 Trigger events

In addition to the scheduled reviews above, if the Firm, through the course of its daily activities, obtains information that brings question to the accuracy of the client due diligence information collected, or if a suspicion arises, then the client will be undergo an immediate review, irrespective of their risk status.

6.6.1 Nominated Officer Reviews

The Nominated Officer will conduct regular independent reviews on accounts opened to ensure that the correct level of due diligence was performed. This will not be required for accounts opened using enhanced due diligence as these will have already been checked/approved by the Nominated Officer. Accounts will be checked to ensure that the appropriate documentation was obtained, a business profile was established, the client was checked for PEPs and Sanctions, and that the client activity matches the expectation from the business profile.

The Nominated Officer will investigate any discrepancies and share any findings with the relevant employees.

6.7 Reporting Suspicious Activities

Employees are expected to be alert to money laundering and they are responsible to make an internal SAR if they notice transactions or behaviour generally that they would subjectively term as suspicious. The completed internal SAR template must be submitted to the Nominated Officer or designee as soon as possible (an in any event within 24 hours).

If suspicious signals of money laundering are identified, the transaction should be frozen and should not proceed without the authorization of the Nominated Officer. All suspicious signals of money laundering are reportable, even if it comes to the employees' attention after the trade has been undertaken or the account is closed, or the trade has been conducted by another person.

Where there is serious suspicion, evidence or reasonable grounds for suspecting, that a transaction may be deemed suspicious, employees are required to report their suspicions in accordance with the Firm's procedures on Suspicious Transaction Reporting.

The Nominated Officer will receive any reports or concerns relating to any suspected or actual money laundering and will record, investigate and report this to the relevant authorities, such as the National Crime Agency (NCA), where necessary. If reports are not forwarded to the relevant authorities, full details of the rationale for this decision will be kept on record.

All notifications made will be handled with strict confidentiality. However, please note that there may be circumstances in which The Firm are required to reveal an individual's identity, for example where we are compelled to do so by law and therefore anonymity cannot be guaranteed.

If there are concerns about any repercussions of making a suspicious transaction report, then the Whistleblowing Policy and Procedure should be followed for information on alternative methods of making a report.

Failure to notify an appropriate person about criminal actions of which an employee is or should have been aware, in breach of this policy, may be considered to be a contractual breach leading to disciplinary actions or personal criminal liability.

6.7.1 Subsequent investigations

The Firm is committed to supporting regulators and law enforcement officers in the prevention of financial crime.

All employees are expected to cooperate fully with any investigations. Employees must also recognise, however, that laws and procedures may apply to the disclosure of information and they should therefore contact the Nominated Officer before disclosing information about clients or employees when contacted directly by law enforcement officers.

6.8 Record Keeping

Records relating to the verification of a client's identity required for the due diligence process will be retained for a period of 5 years after the relationship has ended, or date of one off transaction, after which the personal data will be destroyed, in order to uphold the client's data protection rights. A further period of retention, not exceeding 5 years, will be permitted if after a thorough assessment, the Firm believe this is justified for the prevention, detection or investigation of money laundering or terrorism financing.

The Firm will keep the following records for a period of at least 5 years:

- Customer Identity
- Customer Reviews and evidence of such reviews
- Transaction records (carried out with or for a client)

- Records of any internal reports made to the Nominated Officer and of any external reports made by the Nominated Officer
- Where the Nominated Officer has considered information or other matter concerning knowledge or suspicion that another person has engaged in money laundering, but has not made a report to the National Crime Agency, a record of that information or other matter
- Other records (including but not limited to) Records of training, RBA Assessments, MLRO Reports, quality checking records, policy waivers, oversight and audit findings.

These records are kept at the Firm's offices and the Nominated Officer is responsible for ensuring that these records are complete and up to date.

7 Breaches of Anti-Money Laundering Policy

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

Refer to JMLSG Guidance – *Prevention of money laundering/combating terrorist financing Part II Sectoral Guidance* for sector specific guidance.

8 Annex 1 - Source of wealth and origin of funds information and evidential guide

Description of source of Wealth	Details required	Documentary Evidence required (original or fully certified copy)
1. Income-savings from salary (basic and/or bonus)- if self-employed or company share owner refer to 4 below	All of the following: <ul style="list-style-type: none"> Salary per annum Employer's name and address Nature of Business 	One of the following: <ul style="list-style-type: none"> Payslip (or bonus payment) from the last three months Letter from employer confirming salary on letter-headed paper Bank statement showing clearly showing receipt of most recent regular salary payments from named employer
2. Sale of investment /liquidation of investment portfolio	All of the following: <ul style="list-style-type: none"> Description of shares/units/deposits Name of seller How long held Sale amount Date funds received 	One of the following: <ul style="list-style-type: none"> Investment/savings certificates, contract notes, or surrender statements Bank statements clearly showing receipt of funds and investment company name Signed letter detailing funds from a regulated accountant on letter –headed paper.
3. Sale of Property	All of the following: <ul style="list-style-type: none"> Sold property address Date of Sale Total sale amount 	One of the following: <ul style="list-style-type: none"> Letter from a licenced solicitor or regulated accountant stating property address, date of sale, proceeds received, and name of purchaser Copy of Sale contract
4. Company Sale	All of the following: <ul style="list-style-type: none"> Name and nature of the company Date of Sale Total sale amount Customer's share 	<ul style="list-style-type: none"> Letter detailing company sale signed by a licensed solicitor or regulated accountant on letter headed paper. Copy of contract of sale, plus bank statement showing proceeds Copies of media coverage (if applicable) supporting evidence
5. Inheritance	All of the following: <ul style="list-style-type: none"> Name of deceased Date of death Relationship to customer Date received Total amount Solicitors details 	One of the following: <ul style="list-style-type: none"> Grant of probate (with a copy of the will) which must include the value of estate Copy of will Letter from lawyer or trustee
6. Divorce settlement	Date and total amount received Name of divorced partner	One of the following: <ul style="list-style-type: none"> Copy of the court order Letter detailing divorce settlement signed by a licensed solicitor on letter headed paper

7. Company profits	All of the following: <ul style="list-style-type: none"> Name and address of the company Nature of company Amount of annual profit 	One of the following: <ul style="list-style-type: none"> Copy of the latest audited company accounts Confirmation of the nature of business activity and turnover detailed in a letter from a regulated accountant
8. Retirement income	All of the following: <ul style="list-style-type: none"> Retirement date Details of previous occupation/profession Name and address of the employer Details of pension income source 	One of the following: <ul style="list-style-type: none"> Pension statement Letter from a regulated accountant Bank statement showing receipt of latest pension income and name of provider Savings account statement
9. Fixed Deposits/Savings	All of the following: <ul style="list-style-type: none"> Name and institution where savings account is held Date the account was established Details of how the savings were acquired 	All of the following: <ul style="list-style-type: none"> Savings statement Evidence of account start (letter from the account provider) Additional evidential information can be requested in relation to the origin of the savings held.
10. Dividend payments	All of the following: <ul style="list-style-type: none"> Date of receipt of dividend Total amount received Name of company paying dividend Length of time the shares have been held in the company 	One of the following: <ul style="list-style-type: none"> Dividend contract note Bank statement clearly showing receipt of funds and name of company paying dividend If dividend is payable from the customer's own company, one of the following: <ul style="list-style-type: none"> Letter detailing dividend details signed by a regulated accountant on letter headed paper Set of company accounts showing the dividend details
11. Gift	<ul style="list-style-type: none"> Details of date and amount of gift Details of person making gift – ID and occupation details for PEP/Sanctions screening Reason for gift and the nature of the relationship to the individual making the gift 	<ul style="list-style-type: none"> Letter from donor confirming details of gift If PEP Documented evidence of donor's source of wealth as laid out in this table
12. Loan	<ul style="list-style-type: none"> Name of loan provider Date and amount of loan 	<ul style="list-style-type: none"> Copy of the Loan Agreement and details of any security or, Copy of loan statements
13. Lottery/Gambling Win	<ul style="list-style-type: none"> Name of source Details of Windfall 	<ul style="list-style-type: none"> Evidence from the lottery company Cheque Winnings' receipt
14. Compensation Pay-out	<ul style="list-style-type: none"> Details of events leading to claim 	<ul style="list-style-type: none"> Letter/court order from compensating body or

		<ul style="list-style-type: none">• Solicitor's letter
15. Life Insurance/general insurance pay-out	<ul style="list-style-type: none">• Amount Received• Policy Provider• Policy Number/reference• Date of pay-out	<ul style="list-style-type: none">• Pay-out statement• Letter from insurance provider confirming pay-out