Anti-Money Laundering
&
KYC Policy

RemittVen Ltd.
184 Shepherds Bush Rd, Hammersmith, W6 7NL

History Of Changes To This Document – "Anti-Money Laundering Policy"				
Location of change	**Description of change**	**When**	**Owner**	**Version**

Contents

Introduction

1. About the Manual

This manual takes into account legislative and regulatory requirements as well as recommendations made by the Joint Money Laundering Steering Group (JMLSG) (as amended December 2017). It sets out RemittVen Ltd procedures for due diligence, staff training, reporting and record keeping with a purpose to: enable suspicious transactions to be recognised and reported to the authorities, and; ensure that an audit trail is available to the authorities in the event that anyone who is party to a transaction becomes the subject of an investigation.

The ability to launder the proceeds of crime through the financial systems is vital to the success of criminal operations. The following pages details the specific procedures that can protect RemittVen Ltd from being used by criminals to legitimise their funds through money laundering activity.

2. Background

In the past, efforts to combat money laundering focused on the activities of the banking sector. However, as criminals have adapted to the measures taken by banks over recent years they have now sought other ways to convert illegally earned funds before they enter the banking system, thus making them harder to detect. This has resulted in non-bank financial institutions becoming more vulnerable to being used for money laundering.

There are currently a number of relevant pieces of legislation of which all employees need to be aware including the following:

- The Terrorism Act 2000, and the Anti-terrorism, Crime and Security Act 2001;
- The Proceeds of Crime Act 2002;
- The Serious Organised Crime and Police Act 2005;
- The Money Laundering Regulations 2007;
- Counter Terrorism Act 2008.

The legal definition of money laundering for the purposes of UK legislation is contained in Section 340 of the Proceeds of Crime Act 2002.

2.1 What is Money Laundering?

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins.

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

Examples of Money laundering activity includes:

- Acquiring, using or possessing criminal property;
- Handling the proceeds of crimes such as theft, fraud and tax evasion;
- Being knowingly involved in any way with criminal or terrorist property;
- Entering into arrangements to facilitate laundering criminal or terrorist property;
- Investing the proceeds of crimes in other financial products;
- Investing the proceeds of crimes through the acquisition of property/assets; and
- Transferring criminal property.

There is no single stage of money laundering; methods can range from the purchase and re-sale of luxury items such as a car or jewellery, to passing money through a complex web of legitimate operations. Usually the starting point will be cash but it is important to appreciate that money laundering is defined in terms of criminal property. This can be property in any conceivable legal form, whether money, rights, real estate or any other benefit, if

you know or suspect that it was obtained, either directly or indirectly, as a result of criminal activity and you do not report these suspicions to your MLRO then you too are taking a part in the process.

The money laundering process usually follows three stages:

Placement
Disposal of the initial proceeds derived from illegal activity e.g. into a bank account.

Layering
The money is moved through the system in a series of financial transactions in order to disguise the origin of the cash with the purpose of giving it the appearance of legitimacy.

Integration
Criminals are free to use the money as they choose once it has been removed from the system as apparently "clean" funds.

Please note however that it is rare for any one financial institution to be involved with all stages and as such a firm may only see one or two stages. This makes it harder to detect and prevent as no financial sector business is immune from the activities of criminals and REMITTVEN LTD will consider the money laundering risks posed by the products and services they offer.

2.2 What is Counter Terrorist Financing (CTF)?

Terrorist financing is the process of legitimate businesses and individuals choosing to provide funding to resource terrorist activities or organisations. This could be being done for ideological, political or other reasons. Firms must therefore ensure that:

i. customers are not terrorist organisations themselves; and
ii. they are not providing the means through which terrorist organisations can be funded

There is inevitably some overlap between AML provisions and Terrorist Financing acts. However, there are two major difficulties when Terrorist Financing is compared with other money laundering activities:

i. Often, only quite small sums or money are required to commit terrorist acts
ii. If legitimate funds are used to fund terrorist activities, it is difficult to identify when the funds become terrorist funds

3. Regulatory Framework

There are currently a number of relevant pieces of legislation which REMITTVEN LTD and its employees should be aware of. This chapter will go into the details of the UK regulatory framework.

3.1 Legislation

Within the UK there are a number of legislations which firms need to comply with:

Proceeds of Crime Act 2002 (PoCA) as amended by the Serious Organised Crime and Police Act 2005

- Established a series of criminal offences in connection with money laundering, failing to report knowledge or suspicions or reasonable grounds for knowledge or suspicions, tipping off a person to the fact that a report has been made, and prejudicing an investigation.
- Set out penalties for the various offences established under PoCA.
- Established the Serious and Organised Crime Agency (SOCA) [now integrated into the National Crime Agency NCA], with power to investigate whether a person holds criminal assets, and if so, their location.
- Created five investigative powers for law enforcement.

Under the act the following are money laundering offences:

- **Concealing (Subject to a maximum 14 year jail term and or a fine)**
  Providing assistance to conceal, disguise, convert, transfer or remove funds from the UK if you know, should have known, suspect or should have suspected that the funds were the proceeds of criminal conduct.
- **Arrangements (Subject to a maximum 14 year jail term and or a fine)**
  It is an offence to enter into or become concerned with an arrangement if you know, should have known, suspect or should have suspected that the arrangement facilitates the acquisition, retention, use or control of criminal property.
- **Acquisition, use and possession of funds (Subject to a maximum 14 year jail term and or a fine)**
  Regardless of any attempt to conceal or disguise the criminal origin of property, it is an offence to acquire, use or possess criminal property. Importantly, this offence does not require the laundering process to be actively undertaken.
- **Tipping Off (Subject to a maximum 5 year jail term and or a fine)**
  It is an offence for anyone to take any action likely to prejudice an investigation by informing the person who is the subject of a suspicious activity report, or anybody else, that a disclosure has been made, or that the police or customs authorities are carrying out or intending to carry out a money laundering investigation.
- **Failure to Report (Subject to a maximum 5 year jail term or 2 year jail term in relation to the regulated sector and or a fine)**
  This offence prevents people from turning a 'blind eye' to money laundering by making it a criminal offence for persons working in the regulated sector to fail to report where they have knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering.

The report must be made to the MLRO as soon as reasonably practical after the knowledge, suspicion or reasonable grounds for knowledge or suspicion came to light. There is no defence in claiming no knowledge or suspicion if the circumstances were such that a reasonable person would have known or suspected that the funds could have been the proceeds of crime.

The Money Laundering Regulations 2007 (MLR 2007)
The MLR 2007 applies to institutions who engage in any financial activities. The
MLR 2007 aim to combat money laundering and terrorist financing through:

- Requiring firms to take measures to identity their customers;
- Specifying the policies and procedures that financial institutions and other relevant businesses must put in place in order to prevent and identify activities relating to money laundering and terrorist financing;
- Setting out the supervision and registration arrangements.

Failure to comply with the provisions of the regulations carries a maximum of 2 years imprisonment and or a fine.

Fourth Money Laundering Directive (MLR2017)

The commission published the 4th Money Laundering Directive in June 2015, and this came into effect in June 2017. The regulation and Directive provide a more targeted and focused risk-based approach. In summary, the directive:

- **Extends the definition of politically exposed persons (PEPs) to formally encompass persons entrusted with a prominent public position domestically, as well as domestic PEPs who work for international organisations**

- **Presents a shift to a risk-based approach- removal of the automatic entitlement to apply 'simplified due diligence' (SDD) for specific customers. Instead firms need to carry out risk assessments and provide robust rationale and justification for applying SDD.**
- **Lower the exemptions for one-off transactions and expand the perimeter from €15,000 to €10,000**
- **Include new requirements on beneficial ownership information.**
- **Include tax crimes as predicate offences.**
- **Reinforce sanctioning powers and requirements to co-ordinate cross-border action.**
- **Include national and EU-wide risk assessments.**
- **Include new information requirements for fund transfers.**

Terrorism Act 2000 (TA 2000) as amended by the Anti-Terrorism, Crime and Security Act 2001

- Establishes offences relating to involvement in facilitating, raising, possessing or using funds for terrorist purposes and for failing to report suspicions, tipping off and prejudicing an investigation;
- Empowers authorities to make Orders on financial institutions in connection with terrorist investigations;
- Establishes a list of proscribed organisations with which financial services firms may not deal.

Financial Conduct Authority (FCA) Rules

One of the statutory objectives of the FCA is the enhancement of the integrity of the UK financial system. The statutory objective was derived from the Financial Services and Markets Act 2000 (FSMA 2000). This particular objective incorporates the prevention of money laundering.

The MLRO will provide guidance to you relating to your obligations relating to money laundering and financial crime.

Joint Money Laundering Steering Group (JMLSG)

The JMLSG is made up of the leading UK Trade Associations within the Financial Services Industry. It provides detailed interpretation on the practical issues involved in the implementation of and compliance with the sources of UK legislation outlined above.

3.2 **Penalties**

Apart from the criminal penalties mentioned above, contravention of the laws and rules can also give rise to civil actions under the civil law framework whereby liabilities to the victims of the original crime or subsequent terrorist act could arise.

In addition to risks of prosecution, you also leave your business open to the risk of damage to reputation. Consumers often select financial services firms on the basis of their perceived integrity, trust, ethical standards and professionalism. Perceived involvement in money laundering or terrorist financing could have the effect of destroying a firm's reputation.

3.3 **Apportionment of Responsibilities**

<u>REMITTVEN LTD Responsibility</u>

In order to ensure compliance with obligations under the law, REMITTVEN LTD is required to establish and maintain systems and controls to deter criminals from using their facilities for money laundering purposes.

REMITTVEN LTD's Money Laundering Reporting Officer (MLRO) is Leonardo Romay who has the overall oversight of the firm's anti-money laundering activities, the implementation of appropriate Financial Crime strategies and regulatory reporting obligations.

Staff will direct any queries regarding AML/CTF to the MLRO. All suspicions must be reported to the MLRO. Failure to report your knowledge or suspicions to the MLRO may result in action being taken.

Compliance Monitoring

Leonardo Romay is responsible for ensuring that the firm is provided with compliant and up to date systems and controls policies related to financial crime on a regular basis.

Provisions relating to countries with inadequacies on the approach to Money Laundering Prevention

The HM Treasury may direct any person or institution carrying out relevant business not to enter into a business relationship or carry out one-off transaction, or not to proceed any further with a customer relationship or transaction if the customer is based or incorporated in a country to which the Financial Action Task Force (FATF) has decided to apply counter-measures.

REMITTVEN LTD will make use of national and international findings on countries with inadequacies. This is to enable the Government and Financial Action Task Force findings of inadequacies concerning the approach of money laundering of individual countries or jurisdictions to be brought to bear on the relevant firms' decisions and arrangements.

Responsibility of the staff

All staff working in REMITTVEN LTD, regardless of their actual position, have a duty to be aware of the need to prevent money laundering and terrorist financing.

Should staff have reason to believe or suspect that any transaction, or potential transaction, could involve the proceeds of criminal conduct they must make an internal report of this to its MLRO. Failure to comply with this may result in action being taken upon that staff member.

Responsibility of the Money Laundering Reporting Officer

Leonardo Romay is responsible for the firms Anti-Money Laundering strategy

The MLRO is responsible for:

- Receiving reports relating to (suspicions of) money laundering and terrorist financing;
- Investigating reports of suspicious events;
- Making reports of relevant suspicious events to the NCA;
- Ensuring the adequacy of arrangements made for the awareness and training of all staff and advisers;
- Reporting at least annually to the regulators on the operation and effectiveness of its systems and controls;
- Responding promptly to any reasonable requests for information made by the FCA;
- The approval and assessment of new or amended products/jurisdictions/sales channels and their risks;
- Approving business relationships where the firm wishes to enter or continue a business relationship where the consumer is a Politically Exposed Person, the jurisdiction is considered by Financial Action Task Force (FATF) as non-cooperative or where the country has a high risk of terrorism.

It is the MLRO's overall responsibility to oversee the firm's compliance with the Money Laundering regulations and the FCA Senior Management Arrangements, Systems and Controls (SYSC) Sourcebook.

REMITTVEN LTD's MLRO must report to the National Crime Agency (NCA) any transaction or activity that, after their evaluation, they know or suspect, or have reasonable grounds to know or suspect, may be linked to money laundering or terrorist financing. This is done by means of a Suspicious Activities Report (SAR). Such reports must be made as soon as is reasonably practicable after the information comes to them. REMITTVEN LTD will permit

the MLRO to have access to any information, including 'know your customer' information, in the firm's possession which could be relevant. REMITTVEN LTD's MLRO must consider each report and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion. Any approach to the customer or to the intermediary should be made sensitively and probably by someone other than the MLRO, to minimise the risk of alerting the customer or an intermediary that a disclosure to the NCA may be being considered.

When considering an internal suspicion report, the MLRO will need to strike the appropriate balance between the requirement to make a timely disclosure to the NCA, especially if consent is required, and any delays that might arise in searching a number of unlinked systems and records that might hold relevant information.

Given the need for timely reporting, it may be prudent for the MLRO to consider making an initial report to the NCA prior to completing a full review of linked or connected relationships, which may or may not subsequently need to be reported to the NCA.

The manner of reporting will include typed, paper-based submission on a standard form and the existing electronic submission methods; secure extranet Money Web interface, the NCA's web based reporting mechanism (Suspicious Activity Report) SARs Online, encrypted e-mail or encrypted digital media.

REMITTVEN LTD will include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. In particular, the law enforcement agencies have indicated that details of an individual's occupation/company's business and National Insurance number are valuable in enabling them to access other relevant information about the customer. As there is no obligation to collect this information (other than in very specific cases), a firm may not hold these details for all its customers; where it has obtained this information, however, it would be helpful to include it as part of a SAR made by the firm. If the MLRO decides not to make a report to the NCA, the reasons for not doing so should be clearly documented or recorded electronically, and retained with the internal suspicion report.

MLRO Annual Report

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

- it must assess the relevant firm's compliance with the SYSC Sourcebook and JMLSG Guidance;
- it must indicate the way in which new findings on countries with anti-money laundering inadequacies have been used during the year;
- it must detail the number of internal reports made by staff.

The senior management consider the report and then take any action to remedy any deficiencies identified by the report.

The JMLSG has published a suggested framework to provide information on the MLRO Annual Report. *This document represents a suggested structure for assembling information to enable the MLRO to report on the operation and effectiveness of a firm's systems and controls established to comply with the FCA's Rules - see* http://www.jmlsg.org.uk/other-helpful-material/article/mlro-annual-report

4. Risk Based Approach

REMITTVEN LTD's risk based approach will address the following points:

- identify the money laundering and terrorist financing risks that are relevant to the firm;
- assess the risks presented by the firm's particular
  - customers and any underlying beneficial owners;
  - products;
  - delivery channels;
  - geographical areas of operation;
- design and implement controls to manage and mitigate these assessed risks, in the context of the firm's risk appetite;

- monitor and improve the effective operation of these controls; and
- record appropriately what has been done, and why.

REMITTVEN LTD identifies there is a medium risk that the services they offer can be used for money laundering or terrorist financing, through layering and integration. REMITTVEN LTD does not allow for payments to be made to third parties, and is fully committed to preventing the firm from facilitating financial crime.

REMITTVEN LTD's risk based approach is a stylised categorisation of risk: e.g., high/medium/low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the different treatments of identification, verification, additional customer information and monitoring for each category.

The application of risk categories to customers/situations will provide a strategy for managing potential risks by enabling REMITTVEN LTD to subject customers to proportionate controls and oversight. The key risk criteria are: country or geographic risk; customer risk; and product/services risk.

Before entering into any business relationship, REMITTVEN LTD will have consideration for the following factors:

- Is there a commercial rationale for the customer using the firms services
- Is there a request for a complex or unusually large transaction which has no apparent economic or lawful purpose;
- Requests to associate undue levels of secrecy with a transaction;
- Situations where the origin of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered
- The unwillingness of customers who are not private individuals to give the name of the real owners and controllers

When assessing risk, REMITTVEN LTD will consider all relevant risk factors before determining what the overall risk category is.

Examples of potentially high risk situations as per MLR2017 will include:

Customer risk factors

- Complex business ownership structures, which can make it easier to conceal underlying beneficiaries;
- An individual meeting the definition of a PEP;
- Customer based in, or conducting business in or through, a high risk jurisdiction, or a jurisdiction with known higher levels of corruption;
- Customers engaged in a business which involves significant amounts of cash, or which are associated with higher level of corruption.
- Non –resident customer
- Legal persons or arrangements that are personal asset-holding vehicles
- Companies that have nominee shareholders or shares in bearer form

Country or Geographical risk factors

- Countries identified by credible sources as not having adequate AML/CTF approaches
- Countries subject to sanctions, embargoes, or similar measures issued by, for example to United Nations
- Countries identified by credible sources as having significant levels of corruption or other criminal activity
- Countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country

Product, service, transaction or delivery channel risk factors

- Anonymous transactions
- Non face-to-face business relationships or transactions
- Payment received from unknown or un-associated third parties
- New products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products

Should REMITTVEN LTD wish to enter into a relationship in a high risk jurisdiction or with a PEP or any other high risk scenarios, then prior-approval and guidance must be sought from the MLRO. Failure to comply with this may result in action being taken.

Examples of Lower risk situations include the following:

Customer risk factors

- Other regulated firms and other bodies, where they are subject to requirements to combat money laundering and terrorist financing
- Public companies listed on a stock exchange and subject to disclosure requirements
- Country or geographic risk factors
- Countries identified by credible sources as having effective AML/CTF systems
- Countries identified by credible sources as having a low level of corruption or criminal activity.

Examples of reduced risk products include

- Term life assurance
- Income protection products relating to long term illness
- Critical illness products for a specified critical illness
- Group life protection
- Pensions
- Rebate only personal pension
- pure protection contracts

Based on the risk assessment carried out, REMITTVEN LTD will determine the level of CDD that will be applied in respect of each customer and beneficial owner. Where higher risks are identified, REMITTVEN LTD is required to take enhanced due diligence (EDD) to manage and mitigate the risks. Examples of EDD measures that will be applied for higher risk business relationships include:

- Obtaining, and where appropriate verifying, additional information on the customer and updating more regularly the identification of the customer and any beneficial owner
- Obtaining additional information on the intended nature of the business relationship
- Obtaining information on the source of funds or source of wealth of the customer
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards

REMITTVEN LTD will implement the following risk based assessment for all client:

- a standard information dataset to be held in respect of all customers;
- a standard verification requirement for all customers (CDD);
- more extensive due diligence (more identification checks and/or requiring additional information) on customer acceptance for higher risk customers;

- an approach to monitoring customer activities and transactions that reflects the risk assessed to be presented by the customer, which will identify those transactions or activities that may be unusual or suspicious.

REMITTVEN LTD will document each individual risk assessments in order to be able to demonstrate their rationale for any additional due diligence measures it undertaken or any it has waived compared to the firms standard approach. To add, REMITTVEN LTD will reassess its risk base assessment annually for each individual client, even if the firm decided there is no case for revision. This assessment will be documented in the firm's annual MLRO report.

5. Customer Due Diligence (CDD)

CDD is designed to make it more difficult for the financial services industry to be used for money laundering or terrorist financing. Having sufficient information about your customer and making use of that information is the most effective defence against being used to launder the proceeds of crime.

5.1 What is CDD?

REMITTVEN LTD will carry out CDD and monitoring in order to satisfy themselves that customers are who they say they are, know whether they are acting on behalf of another, and that there is no legal barrier to providing them with the product or service requested and to enable the firm to assist law enforcement, by providing available information on customers or activities being investigated.

Overview of CDD measures:
REMITTVEN LTD will be able to demonstrate that it is:

- Identifying the customer, and verifying their identity;
- Identifying the beneficial owner, where relevant, and verifying their identity; and
- Obtaining information on the purpose and intended nature of the business relationship.

It may often be appropriate for REMITTVEN LTD to know rather more about the customer than their identity: it will, for example, often need to be aware of the nature of the customer's business in order to assess the extent to which their transactions and activity undertaken with or through the firm is consistent with that business.

REMITTVEN LTD must apply CDD measures when it:

- Establishes a business relationship;
- Carries out an occasional transaction;
- Suspects money laundering or terrorist financing; and
- Doubts the veracity of documents, data or information obtained for the purpose of identity verification.

Know Your Customer

When a business relationship is formed, in order to establish what might constitute normal activity later in the relationship, it is necessary for REMITTVEN LTD to ascertain the nature of the business a client expects to conduct.

Once an on-going business relationship has been established, any regular business undertaken for that customer can be assessed against the expected pattern of activity of the customer. Any unexplained activity can then be examined to determine whether there is a suspicion of money laundering or terrorist financing.

Information regarding a client's income, occupation, source of wealth and the economic purpose of any transaction is typically gathered as part of the provision of service. At the start of the relationship personal information is also obtained, such as, nationality, date of birth, and residential address. These pieces of information should also be considered in respect to the risk of financial crime (including AML and CTF). For high risk transactions it might be appropriate to seek verification of the information the client has provided.

Source of Funds

When a transaction takes place, the source of funds, i.e. how the payment is to be made, from where and by who, must always be ascertained and recorded in the client file (this would usually be achieved through retaining a copy of the cheque or direct debit mandate).

5.2 Simplified Due Diligence (SDD)

SDD means not having to apply CDD measures; in practice, this means not having to identify the customer, or to verify the customer's identity, or, where relevant, that of a beneficial owner, nor having to obtain information on the purpose or intended nature of the business relationship. It is, however, still necessary to conduct ongoing monitoring of the business relationship.

As per MLR2017, REMITTVEN LTD will ensure that SDD is now individually assessed and there will be no automatic entitlement to apply SDD. Therefore, SDDwill depend on the type of customer, the type of product, the size of the transaction and the geographical risk factors.REMITTVEN LTD will apply SDD after determining that the business relationship or transaction presents a lower degree of risk.
SDD may be applied to:

i. Companies listed on a regulated market;
ii. Where the applicant itself is authorised to undertake UK financial activity under FSMA 2000, or is a non-UK financial sector firm covered by the Money Laundering Directive, or is undertaking regulated financial sector activities in a country with equivalence status – this can be confirmed on FATF's website;
iii. Beneficial owners of pooled accounts held by notaries or independent legal professionals;
iv. UK public authorities;
v. Community institutions;
vi. Certain life assurance and e-money products;
vii. Certain pension funds;
viii. Certain low risk products;
ix. Child trust funds/Junior ISAs; and
x. One off transaction exemption can apply where the payment to be made by or to the applicant is less than €15,000. Further services by you would constitute a business relationship upon which full verification will be sought.

Please note that the exemptions from the identification procedures for customers are all subject to the overriding condition that there is no knowledge or suspicion on the part of the firm or its employees, or no reasonable grounds for knowing or suspecting, that the customer, or any person on whose behalf the customer is acting, is engaged in Money Laundering.

5.3 Enhanced Due Diligence (EDD)

REMITTVEN LTD will apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, REMITTVEN LTD may conclude, under its risk based approach, that the standard evidence of identity is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer. REMITTVEN LTD may take more intrusive and exhaustive steps to0 establish not only the source of funds but also the source of wealth.

The extent of additional information sought, and of any monitoring carried out in respect of any particular customer, or category of customer, will depend on the money laundering or terrorist financing risk that the customer, or category of customer, is assessed to present to the firm.

Examples of when EDD needs to be applied include:

i. Where the consumer has not been physically present for identification purposes
ii. Transactions involving Politically Exposed Persons
iii. Where a product is considered by its nature to be higher risk
iv. Where a consumer is from a high risk jurisdiction

5.4 Keeping Due Diligence information up to date

Where information is held about customers, it must, as far as reasonably possible, be kept up to date, which may be done by completing a new form as often as necessary. Once the identity of a customer has been verified there is no obligation to re-verify it, unless suspicion dictates otherwise, however, it is necessary to ensure customer information such as, personal and financial circumstances, change of address or employment etc. is kept up to date under MLR 2007.

6. Know Your Customer – The Basis for Recognising Suspicions

A suspicious transaction will often be a transaction which is inconsistent with the customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognise that a transaction, or series of transactions, is unusual.

6.1 **Things to consider**

In order to determine whether an established customer's transaction might be suspicious REMITTVEN LTD will consider:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?
- Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

6.2 **Suspicious Scenarios**

Issues which will cause suspicion would include:

- Business terms that appear too good to be true, for example the offer of fees that seem disproportionate to the work being undertaken;
- Clients who are reluctant to provide proof of identity;
- Clients who place undue reliance on an introducer (they may be hiding behind the introducer to avoid giving you a true picture of their identity or business);
- Requests for cash related business, for example questions about whether investments can be made in cash, suggestions that funds might be available in cash for investment;
- Linked transactions which might be being used to disguise or divert money, for example unnecessary switching, encashment and reinvestment of the same funds, possibly in the name of a partner, business or family member;
- Where the source of funds for investment is unclear;
- Where the magnitude of the available funds appears inconsistent with the client's other circumstances (i.e. the source of wealth is unclear). Examples might be students or young people with large amounts to invest;
- When a transaction does not appear to make sense given the client's circumstances, particularly if the client insists on following such a route against your advice. (Care should be taken not to automatically include all insistent clients within this idea. A weight of suspicious evidence leading to a genuine suspicion is what you should be looking for);
- Where the transaction doesn't appear rational in the context of the customer's business or personal activities. Particular care should be taken in this area if the client changes their method of dealing with you without reasonable explanation (e.g. from advisory to execution only);
- Where the pattern of transactions changes;
- Where a client who is undertaking transactions that are international in nature does not appear to have any good reason to be conducting business with the countries involved (e.g. why do they hold monies in the particular country that the funds are going to or from? Do their circumstances suggest that it would be reasonable for them to hold funds in such countries?);
- Where lump sum investments are used by the investor as security for loans; and
- Clients who are unwilling to make face-to-face contact, or to provide you with normal personal or financial information, for no apparent or rational reason. (Care should be taken not to include all

distance relationships as suspicious, because most will be for genuine reasons. Suspicions will ordinarily be based upon cumulative as opposed to stand alone issues).

REMITTVEN LTD is aware that a money launderer is likely to provide persuasive arguments about the reasons for their transactions. REMITTVEN LTD will therefore look behind these, at the client's actual circumstances, to decide whether a transaction is suspicious.

Any suspicions must be reported promptly to the MLRO in accordance with clearly laid down procedures. This will protect staff from any future recourse including prosecution.

6.3 **Cancellation / Cooling Off & General Surrenders of Plans**

The cancellation, cooling off or early encashment of investments provides a readily available route for laundering money and REMITTVEN LTD will be aware of any unusual activity of this kind.

In particular, REMITTVEN LTD will be alert to the following:

- Requests to pay surrenders to third parties;
- Surrenders of plans in the short term, especially if this involves monetary loss;
- Surrenders which do not appear rational given your knowledge of the client's circumstances;
- Early surrender of plans where the available "know your customer" information is lacking (for example due to the business being placed "execution only", by direct offer or because the client refused to disclose fact find information at outset);

Each of the above points will be considered whenever you are requested to action or become aware of the surrender of a plan. A report to the MLRO will be made if any employee of REMITTVEN LTD has any concerns.

7. **Recognising Suspicious Transactions**

Where you have knowledge or a suspicion that an individual or business is engaged in money laundering or terrorist financing you must make a report to the MLRO. Failure to report your knowledge or suspicions to the MLRO may result in action being taken.

Knowledge for the context of this section is defined as a degree of satisfaction, not necessarily amounting to belief, at least extending beyond speculation, as to whether an event has occurred or not. Knowledge can be categorised as:

- Actual knowledge;
- Wilfully ignoring the obvious;
- Wilfully and recklessly failing to make such enquiries as a reasonable and honest person would make;
- Knowledge of other circumstances.

7.1 **Reporting a Suspicion**

Where, for whatever reason, you suspect that a client, or anybody for whom they are acting, may be undertaking (or attempting to undertake) a transaction involving the proceeds of any crime you must report your suspicion to the MLRO as soon as practicably possible and in writing.

Internal reports to MLRO must be made regardless of whether the business has actually taken place. In some instances it may be necessary for the MLRO to obtain consent from the National Crime Agency (NCA) prior to being able to continue with the transaction.

Making a Report

The internal suspicions report must be made as soon as reasonably possible to the MLRO and the following process will be followed:

- An internal suspicious report will be completed and submitted to the MLRO. The report will provide full details of the client and a full statement of the circumstances giving rise to the suspicion, as a minimum:
    - Details of all parties to the transaction;
    - The owner of the monies in question;
    - How the identity of the client was verified;
    - A full description of the transaction;
    - Reasons for suspicion and supporting evidence.
- This will be forwarded, together with any supporting documentation to the MLRO immediately.
- Your suspicion report will be acknowledged, and a response will be provided by the MLRO (along with a reminder of the obligation to do nothing that might prejudice enquiries - i.e. tipping off).
- If for any reason you do not receive an acknowledgement you should contact the MLRO.

Please send the completed internal suspicions report to Leonardo Romay.

Once you have reported your suspicion to the MLRO you will have satisfied your statutory obligation. It is unlikely that the MLRO will be able to provide you with any details in relation to the outcome of your report and you should not ask them to do so. In the event that further suspicion arises after a report has been made to the MLRO a further report should be made.

Where required the MLRO will forward the report and concerns to the National Crime Agency (NCA) for consent to proceed. In such circumstances, it is an offence to consent to a transaction or activity going ahead within the seven working day notice period from the working day following the date of disclosure, unless the NCA gives consent. Where urgent consent is required, requests should be transmitted electronically over a previously agreed secure link or by a communication method as specified on the NCA website at www.nca.gov.uk.

When an activity or transaction (or a related transaction) which gives rise to concern is already within an automated clearing or settlement system, where a delay would lead to a breach of a contractual obligation, or where it would breach market settlement or clearing rules, the nominated officer may need to let the transaction proceed and report it later. Where the nominated officer intends to make a report, but delays doing so for such reasons, POCA provides a defense from making a report where there is a reasonable excuse for not doing so. However, it should be noted that this defence is untested by case law, and would need to be considered on a case-by-case basis.

7.2 **Protection from Prosecution**

Staff are reminded that only by ensuring an internal report is made to the MLRO will they protect themselves from future prosecution.

No protection would be offered by simply making a report to your own practice or line manager. It is important to ensure your suspicions/report have reached the correct person.

REMITTVEN LTD will consider disciplinary action against any member of staff who fails, without good reasons to make a report of the kind envisaged. Further guidance in this event should be sought from the Nominated Officer or MLRO.

Customer Confidentiality and Reporting of Suspicions

The money laundering legislation protects those reporting suspicions of money laundering from claims in respect of any alleged breach of customer confidentiality.

Where cooperating with the MLRO in its investigations

If you make a report to the MLRO which leads to an investigation into a potential case of money laundering, it is likely that before taking a decision as to whether or not to make a report to the authorities, the MLRO will need access to all information in the firm's possession. In particular documentation relating to the financial circumstances and transactions of a client or any person on whose behalf the client has been acting. Where requested by the MLRO or the authorities this information should be made readily available.

Ending a Business Relationship

Before ending a business relationship with a client for whom you have made an internal suspicion report you should contact the MLRO for guidance on how to do so.

Reporting Overseas Offences

For money laundering offences to be committed laundering must take place in the UK. However, the offence of failing to report that another person is engaged in money laundering also applies to money laundering abroad where this would amount to a money laundering offence if it took place in the UK. Consequently, in the event that money laundering committed abroad comes to the attention of a person whilst undertaking business within the UK it should be reported to the MLRO.

Freezing of Accounts

Where REMITTVEN LTD knows that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account must be frozen. Where it is believed that the account holder may be involved in the fraudulent activity that is being reported, then the account may need to be frozen, but the need to avoid tipping off would have to be considered.

8. Type of Client

8.1 Private Individuals: Face-to-Face

Identification

The standard identification requirement for customers who are private individuals are generally governed by the circumstances relating to the customer and the product type that is being dealt in, i.e. the level of risk attributed to the product whether it is a reduced risk, intermediate risk or an increased risk product.

Where the customer is purchasing a reduced risk and intermediate risk product the following pieces of information are required as a standard for identification purposes:

- Full Name
- Residential Address
- Date of Birth

Verification

Verification of the information obtained must be based on reliable and independent sources – which might either be documents provided by the customer, or electronically by a firm, or by a combination of both. Where business is conducted face-to-face, firms should see originals of any documents involved in the verification.

If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the firm reasonable confidence in the customer's identity, although REMITTVEN LTD will weigh these against the risks involved.

Government Issued photographic Documents should incorporate:

- The customer's full name, and either their:
    - residential address; or
    - date of birth

Accepted forms of Government Issued photographic Identity documents:

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

Alternatively, this can be done by a non-photographic government issued document which incorporates the customer's full name, supported by a second document, which incorporates:

- The customer's full name, and either their:
    - residential address; or
    - date of birth.

Non-Photographic Government Issued Identity Documents:

- Valid full non-photographic UK Driving Licence (may be used as proof of address or identity but not both);
- State Pension / Benefits Book or Notification Letter (may be used as proof of address or identity but not both);
- Sub-contractors Certificate;
- HMRC Tax Notification (P45 or P60 may not be used);
- Resident Permit issued to EU Nationals by Home Office;
- Identity Card (EEA members and Switzerland only);
- Local Authority Tax Bill.

Evidence of Address

- Current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK, EU or an equivalent jurisdiction (but not ones printed off the internet or dated more than three months ago);
- House or motor insurance certificate;
- Utility bills (not including mobile phone bills, not ones printed off the internet or bills dated more than three months ago);
- Current council tax demand letter or statement, rent card or tenancy agreement;
- Home visit (premises must be entered);
- Solicitor letter confirming completion of house purchase or land registration (certified copy);
- Electoral role check (certified copy);
- State Pension or Benefits Book (may be used as proof of address or identity but not both);
- Valid UK driving licence (may be used as proof of address or identity but not both).

For increased risk level products, in addition to obtaining the standard information detailed above, the following should also be obtained and recorded:

- Employment and income details
- Source of wealth (i.e. source of the funds being used in the transaction)

Non-Government Issued Identity Documents

Non-government-issued documentary evidence complementing identity should normally only be accepted if it originates from a public sector body or another regulated financial services firm, or is supplemented by knowledge that the firm has of the person or entity, which it has documented.

It is recommended that you take copies of the documents used for verification whenever possible (e.g. when seeing a client in your office or where copying facilities are available).

Whenever you take copies of identification evidence these must be dated and signed "original seen".

Where a copy of evidence taken includes a photograph you must also certify that the photograph provides a good likeness of the client by writing on the photocopy "the photograph is a good likeness of the applicant".

Where a new residential address cannot be proved, because the address is only temporary or because verification evidence is not yet available, then the previous address should be verified. The current address should be verified as soon as practically possible afterwards. Notes should be held on file to clarify the situation.

Electronic Verification

REMITTVEN LTD use RemitOne for Electronic Verification. REMITTVEN LTD is to be satisfied that information supplied by RemitOne as a software provider for our SPI, phonetic checklist is included on their scope of services is sufficiently extensive, reliable and accurate.

8.2 Private Individuals: Non-Face-to-Face

Non Face-to-Face due diligence applies to any client who you are not meeting in person. This is because non face-to-face transactions pose a greater risk than those conducted in person because it is more difficult to be sure that the person with whom you are dealing is the person that they claim to be. Therefore, this type of customer would qualify for an enhanced due diligence check.

REMITTVEN LTD will therefore apply an additional verification check to manage the risk of impersonation fraud. The additional check will include one or the following:

- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise),
- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);
- requiring copy documents to be certified by an appropriate person.

UK Nationals

Certification of Identity documents of UK nationals can be undertaken by a regulated or professional person covered by the money laundering regulations or by somebody from a government department/agency or organisation. This means that the documentation could be certified by one of the following people:

- Accountant
- Authorised Financial Intermediary
- Banker
- Civil Servant
- Doctor
- Solicitor
- Teacher
- Other qualified Individuals

Non-UK Nationals

The same procedures would apply for customers who are Non-UK Residents and wish to solicit services on a remote basis however; the identity documentation in this case may be certified only by the following:

- An embassy, consulate or high commission of the country of issue; or
- Lawyer or attorney; or
- For international students, only by staff in the registry of a UK higher education institution.

The regulations require, where business is being conducted on a non face-to-face basis, additional checks to guard against identity fraud should be conducted.

8.3 Non UK Nationals and / or Residents

Dealing with non UK nationals and/or residents can lead to a greater and in some cases significant risk of financial crime. You must always consider whether there is a legitimate reason for them to be undertaking transactions in this country and with yourself. If you cannot identify such reasons, this is cause for suspicion and you should make an immediate report to the MLRO.

You should remain mindful at all times that verification of identity checks must be completed prior to conducting business and that failure to follow these procedures may possibly lead to a criminal offence being committed.

Particular care should be taken when the business relationship involves links to jurisdictions with AML / CTF Frameworks not comparable to that of the UK (EEA Members, United States of America, Canada and Australia are considered to have comparable AML /CTF Frameworks).
Meeting with these requirements may lead to a delay in your ability to action transactions for the client. Thus, when dealing with non-UK residents, you should make them aware of your obligations under the prevention of money laundering legislation and manage their expectations accordingly.

In accordance with a risk based approach to anti-money laundering processes, when verifying prospective customers who are non-UK residents and / or nationals, the standard verification is considered to be insufficient. Single document verification should not be permitted. Instead the following due diligence should be conducted:

Source of Funds:

- Evidence of the source of funds should be obtained and the information recorded. Consideration should be given to the jurisdiction from which the funds are originating. If the funds are coming from outside of the UK then approval from the MLRO should be requested.

Proof of Name:

- Evidence of name should be taken through sight of an original passport or national identity card only;
- Copies of the pages containing reference numbers, date and country of issue, Visas and travel stamps should be taken;
- In circumstances where taking copies of these pages is not possible you must ensure that you record all of this information on your file.

Proof of Address:

- Evidence of the client's permanent (overseas) address should be obtained;
- This should be the best available and must be from an official source (e.g. government agency or bank or credit institution);
- Such evidence may be obtained directly from the customer (i.e. sight of original correspondence from one of these agencies/institutions to the client at their permanent address in the last 3 months) or may be a confirmation of address received directly from these bodies;
- Where the confirmation of address is received directly this document should be retained;
- Where sight of documentation is provided by the client you should take copies of this whenever possible. Where this is not practical you must note the name and type of the institution, the date of issue, the details of the address and any associated reference numbers;
- Should you have any doubt about the authenticity of the documentation provided you should inform the MLRO immediately of your doubts.

Know Your Customer

- The following information should also be obtained and recorded:
    - Employment and income details
        - The client's employment is their job title and their income should include income from all sources.
    - Source of wealth
        - Source of wealth is the source from which the client accumulated the funds being used in the transaction e.g. lottery win, inheritance, disposable income, matured investment etc.

8.4 **Recently arrived Non-UK Nationals**

If the client is a non-UK national and has arrived in the UK in the last three months an additional check must be carried out by contacting their employer (or place of education) to corroborate their identification and permanent residential address. You may do this either by telephone or in writing (written evidence is preferred). You are likely to require the client's authority before the employer or educational institution will release such information.

Home Office confirmation should be sought verifying that the client has permission to be in the UK. A copy of a work permit would be sufficient for this purpose.

8.5 **Customers who cannot provide the required documentation**

On occasions you may be approached by clients who are unable to provide the documents detailed above, (e.g. they don't have a passport or driving licence and their name doesn't appear on utility bills). Clearly there are special circumstances for verifying the identity of certain categories of people for example the mentally incapacitated, asylum seekers, economic migrants, prisoners, those on probation, some students and minors.

In many of these cases it will be possible to arrange to collect a number of alternative documents to build up a suitable "weight of evidence" to satisfy the MLRO that the client is who they claim to be. If you are dealing with higher risk clients you must seek approval from the MLRO prior to entering into the business relationship.

Where alternative documentation is not available you should undertake the "Financial Exclusion" verification process in full.

Financial Exclusion Process

Where the client is genuinely unable to provide proof of identity documentation, and provided they are a UK resident, you may accept as identification evidence a letter or statement from a person in a position of authority who knows the client. The JMLSG has issued guidance which highlights the following individuals as being suitable for this purpose:

- UK Solicitors;
- Doctors;
- Hostel managers/ social workers;
- District Nurse/ Midwife;
- Teacher;
- Care home managers;
- Minister of religion;
- Prison governors/ probation officers;
- Police officers;
- Civil servants;
- Members of Parliament;
- Local/county councillor.

The letter must:

- Confirm that the client is who they claim to be;
- Confirm their permanent address;
- Be personally signed by the person in authority;
- Include the writer's address and preferably be on headed note paper;
- Contain a contact telephone number for the person in authority.

Required Confirmation Action

On receipt of the letter you should contact the person in authority (telephone contact would be sufficient for this purpose) to confirm that they provided the letter and that the details contained within it are correct. You must include a note within the client file explaining why the financial exclusion rules were utilised.

Caution should be exercised when applying the Financial Exclusion process. You should consider the applicant's circumstances and satisfy yourself that it is reasonable that the applicant is unable to provide the necessary verification of identity documentation. If their circumstances suggest that such information should be available, their unwillingness to provide it should cause you to be suspicious and you should report this to the MLRO.

Corporate Customers

Corporate customers may be publicly accountable in several ways. Some public companies are listed on stock exchanges or other regulated markets, and are subject to market regulation and to a high level of public disclosure in relation to their ownership and business activities. Other public companies are unlisted but are still subject to a high level of public disclosure through public filing obligations. Private companies are not generally subject to the same level of disclosure, although they may often have public filing obligations. In their verification processes, firms should take account of the availability of public information in respect of different types of company.

Control over companies may be exercised through direct or indirect shareholdings in companies. REMITTVEN LTD will establish the controllers and beneficial owners of the company where necessary, this will depend on the nature of the company, the distribution of shareholdings, and the nature and extent of any business or family connections between the beneficial owners.

8.6 Public Registered Companies

Public Limited Companies listed on regulated markets are generally held publicly accountable through high levels of public disclosure and high levels of market regulation in relation to their ownership and business activities. Unlisted Public Limited Companies are not generally subject to market regulation but are still subject to high levels of public disclosure through public filing obligations. As a result, the verification process for these companies is generally low level in comparison to other business entities. The firm should understand the company's legal form, structure and ownership, and obtain information on the nature of the company's business, and the reasons for seeking the firm's product or service.

Companies Listed on a Regulated Market

PLCs that are listed on a regulated exchange in an EEA state or a non-EEA state may be subject to disclosure obligations consistent with specified articles. These Disclosure obligations are contained within the following articles:

- The Prospectus directive [2003/71/EC]
- The Transparency Obligations directive [2004/109/EC]
- The Market Abuse directive [2003/6/EC]

REMITTVEN LTD can apply Simplified Due Diligence procedures where it has verified that:

- the individual the firm is dealing with has authority to act on behalf of the company (customer)
- The company is listed on a regulated market (within the meaning of MiFID) in an EEA state and is subject to specified disclosure obligations (see above) (for a company listed on the LSE for example, the SEDOL number of the firm and the exchange the firm is trading would be satisfactory)

A record should be kept of the steps the firm has taken to establish the above points.

If the market is based outside the EEA and subjects its listed companies to disclosure obligations that are contained within the International Standards and are equivalent to the specified disclosure obligations in the EU, similar treatment as the above is permitted.

Companies that are not located within the EEA and do meet the above requirements are subject to the standard verification requirement for private and unlisted companies (see later).

In order to ascertain whether the individual acting on behalf of the company is authorised to do so one of the following will be carried out:

- Obtain a copy of the board resolution giving the individual authority to act;
- Obtain confirmation from the legal department of the firm that the individual is authorised to act
- Call the company from an independently verified number (e.g. form a phone book) and check the individual's credentials with a third party at the firm. The client may need to be informed that the check is a part of procedures
- In the case where a director of the firm has written to a firm in respect of a transaction on company letter headed paper, then that in itself should satisfy the requirement.

Regardless of the above, the following will be obtained as a standard in relation to all listed companies:

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

Majority Owned and Consolidated Subsidiary

Where it is the case that a company is majority owned or is a subsidiary of a company listed on a regulated market, simplified due diligence may be applied. However, independent confirmation should be obtained to verify that the company is a subsidiary of, or is majority owned by the parent company.

Unlisted PLCs and Limited Liability Partnerships (LLPs)

Unlisted public registered companies though not subject to the level of public disclosure equivalent to listed companies are still subject to high levels of public disclosure. For these types of companies a firm should obtain the following information as a standard:

- Full name
- Registered number
- Registered office in country of incorporation
- Business address
- Names of all directors (or equivalent)
- Names of beneficial owners who own or control over 25% of its shares or voting rights
- Confirmation that the individual the firm is dealing with has authority to act on behalf of the company (customer)
- Existence of the corporate body has to be verified (this can be done by obtaining a copy of the company's Certificate of Incorporation of equivalent)

In order to ascertain whether the individual acting on behalf of the company is authorised to do so one of the following will be carried out:

- Obtain a copy of the board resolution giving the individual authority to act;
- Obtain confirmation from the legal department of the firm that the individual is authorised to act
- Call the company from an independently verified number (e.g. form a phone book) and check the individual's credentials with a third party at the firm. The client may need to be informed that the check is a part of procedures
- In the case where a director of the firm has written to a firm in respect of a transaction on company letter headed paper, then that in itself should satisfy the requirement.

In the case of higher risk transactions, i.e. when dealing with 'increased risk products' or country then the following should be verified also on a risk based approach:

- Any entities directly or indirectly with a beneficial interest of 25% or more
- Any entity authorised to give instructions to move assets or funds (e.g. signatories)

This could be done by the obtaining a letter of confirmation from the company secretary of the parent company or through obtaining a copy of the annual reports from the parent company which make reference to the subsidiary.

REMITTVEN LTD will retain awareness of changes to beneficial ownership that might occur over time. If REMITTVEN LTD was to carry out further transactions for the same company, we will strive to identify any such changes and ensure that new shareholders or beneficial owners are verified where necessary.

Where the individual with whom you are dealing does not appear on the list of directors that you obtain, you should verify that the individual with whom you are dealing is authorised to act.

Private Limited companies

Unlike publicly quoted companies, the activities of private or unlisted companies are often carried out for the profit/benefit of a small and defined group of individuals or entities. Such firms are also subject to a lower level of public disclosure than public companies.

In the UK, a company registry search will be conducted to confirm that the applicant company has not been, or is not in the process of being, dissolved, struck off or wound up. In the case of non UK companies, similar search enquiries of the registry in the country of incorporation of the applicant for business will be conducted..

Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, REMITTVEN LTD will consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identities of other shareholders and/or controllers.

As part of the standard evidence, the firm will know the names of all individual beneficial owners owning or controlling more than 25% of the company's shares or voting rights, (even where these interests are held indirectly) or who otherwise exercise control over the management of the company.

REMITTVEN LTD will obtain the following in relation to the corporate concerned:

- full name
- registered number
- registered office in country of incorporation
- business address
- names of all directors (or equivalent)
- names of individuals who own or control over 25% of its shares or voting rights
- names of any individual(s) who otherwise exercise control over the management of the company.
- The identity of the Beneficial Owner as a Legal Person.

Following REMITTVEN LTD's assessment of the money laundering or terrorist financing risk presented by the company, it will, using GBG ID3 Global, verify the identity of individuals owning or controlling more than 25% of the shares or voting rights. It will also verify the identity of the Beneficial owner verify the identity of one or more directors, as appropriate, in accordance with the guidance for private individuals. Verification is also likely to be appropriate for those who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets.

<u>Bearer shares</u>

Extra care must be taken in the case of companies with capital in the form of bearer shares, because in such cases it is often difficult to identify the beneficial owner(s). Companies that issue bearer shares are frequently incorporated in high risk jurisdictions. REMITTVEN LTD will adopt procedures to establish the identities of the holders and material beneficial owners of such shares and to ensure that they are notified whenever there is a change of holder and/or beneficial owner.

8.7 **Sole Traders and Partnerships**

Sole trader and partnerships are subject to a lower level of public disclosure than private limited companies or a limited liability companies, as a result, the degree of due diligence required will be proportionally higher.
When the customer is an unincorporated business such as a sole trader or a partnership, the following verification of identity checks will be carried out:

- Each partner/beneficial owner must be verified (as a private individual);
- Any individual not in the above group who has the ability to control the investment or product (e.g. signatories) must be verified (as a private individual);
- Obtain evidence of the trading address through sight of an original bank statement or utility bill, less than 3 months old, in the name of the unincorporated business.
- Names of individuals who own or control over 25% of its capital or profit, or of its voting rights. The firm must take risk based and adequate measures to verify the identity of those individuals

For identification purposes, Scottish partnerships and limited liability partnerships should be treated as corporate customers. For limited partnerships, the identity of general partners should be verified whilst other partners should be treated as beneficial owners.

You should also satisfy yourself as to the purpose of the partnership/business and the activities they undertake. Where a formal partnership arrangement is in place, sight of this should be obtained. In addition, the firm should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer

8.8 **Business introduced or transferred from another client**

The responsibility to obtain satisfactory evidence rests with REMITTVEN LTD. The firm may reasonably rely on another FCA regulated firm to:

- Undertake the identification procedures when introducing a client to you; or
- To confirm the identification details if the client is not resident in the UK.

8.9 **Business introduced from another regulated firm**

REMITTVEN LTD MUST obtain a copy of the Confirmation of Verification of Identity (CVI) Form completed by the other regulated firm. This will be accompanied by certified copies of the documentation.

REMITTVEN LTD will only rely on the other regulated firm if the documentation provided is such that it would meet the firm's internal procedures as documented in this policy document.

REMITTVEN LTD will still need to complete a standard CVI Form on submission of a proposal to the product provider.

If you have reasonable grounds to doubt the authenticity of any information provided, REMITTVEN LTD will carry out its own verification checks.

Acquiring another firm or portfolio of clients

When a firm acquires the business or clients of another firm it is not necessary to re-verify the identity of all the customers provided that:

- All underlying customer records are acquired with the business; or
- A warranty is given by the acquired firm or by the vendor where a client bank or business has been acquired, that clients have been identified.

Notwithstanding the above, it is expected that the acquiring firms due diligence enquires include provision to conduct sample testing in order to confirm the identification procedures previously applied were robust and adhere your firm's own standards.

8.10 **Pension Schemes**

New Business

The exact requirements for money laundering verification when arranging pension transactions depends upon the type of pension contract and the source of the premiums.

The specific requirements for pension business are described below:

Contract Type	Verification Requirements
Reduced Risk	
Rebate Only Pension	Obtain HMRC notification form for the individual
Contracted in Money Purchase Schemes, Contracted out Money Purchase Schemes Final Salary Schemes Group Additional Voluntary Contribution Plans	No verification required provided they have exempt approval status from HMRC.
Intermediate Risk	
Group and Individual Personal Pensions (GPP), Group and Individual Stakeholder Pensions, Income Drawdown Flexible Pension Plan, Phased Retirement Plans, Immediate Vesting Personal Pension	If premiums paid via employer only (for example payroll deduction) employer Verification of Identity only required; If premium paid also or only by employee (for example by direct debit or by additional lump sum payments), employee Verification of Identify required. All third party payers should be verified
Compulsory Purchase Annuity; Open Market Option; With Profit Pension Annuity.	If the funds are from an approved Occupational Pension Scheme or regulated Financial Services scheme then no verification is required. If the funds are from another source the annuitant must be verified.
Increased Risk	
Executive Pension Plan	Employer; Beneficial trustees or those who may give instruction (if FCA regulated then record their FCA number); Third party payers.
Small Self Administered	Employer; Beneficial trustees or those who may give instruction; Beneficial pensioner trustees or those who may give instruction. ID Verification also required if they are not on the HMRC pensioner trustee approval list; Third party payers.
Self Invested Personal Pension	Policy holder; Employer; Third party payers.
TIPPS	Trustees, if FCA regulated then record their FCA number. Party giving payment instructions where a TIPP is held on behalf of a SSAS managed by another firm unless that firm is regulated or payment can only be made by a regulated firm.

8.11 **Reduced Risk Level Products**

There is no requirement to verify identity if the transfer is from an occupational pension scheme which:

- Is not an Executive Pension Plan (EPP) or a Small Self Administered Scheme (SSAS);
- Is to an Occupational Scheme which is not an EPP, SSAS or a Section 32 (S32), with no additional funding.

8.12 **Intermediate Risk Level Products**

The verification requirements are where there is a transfer with ongoing contributions to verify:

- The employer, if premiums are paid via the employer; and
- The employee, where contributions are also, or only, paid direct by the employee i.e. from the personal bank account; and
- Any third party payers

If the pension transfer is literally just a change of product provider with no additional contributions being made at that time no verification of identity is necessary.

Increased Risk Level Products

Refer to the verification of identity requirements as detailed for increased risk products in the above table. Again, if the transfer merely involves a change of provider with no additional contributions then a verification of identity is not necessary.

8.13 **Clubs & Societies**

When conducting business for a club or society the following steps will be taken to verify its identity:

- REMITTVEN LTD must satisfy itself as to the legitimate purpose of the organisation. This could be by obtaining sight of its constitution; and
- At least two of the club or society contacts should be verified as private individuals.

For investment clubs (i.e. those whose purpose is to purchase regulated investments) all members should be considered as individual clients and verified accordingly.

8.14 **Charities in England & Wales**

The verification rules in respect of charities have two purposes:

- To prove that the charity actually exists; and
- To demonstrate that the individual with whom you are dealing is authorised to act for the charity.

This can be achieved as follows:

- The existence of the charity can be verified by checking with the charity commission of England and Wales, this can be done online (http://www.charity-commission.gov.uk) or for Scottish charities, the Office of the Scottish Charity Regulator website (www.oscr.org.uk), Northern Ireland Charites can be verified through the Northern Irish Charity Commission (http://www.charitycommissionni.org.uk/charity-search/)
- The charity commission should also be able to provide details of the charity's "correspondent". If the person undertaking the transaction is the named correspondent then no further verification is required; and
- In cases where the person undertaking the transaction is not the correspondent you should also forward a copy of the suitability letter to the designated correspondent. A covering note should also be included to cover the details of the transaction in brief and request the designated correspondent to contact you should all not be in order.

The firm must obtain the following information in relation to charities:

- Full name and address
- Nature of body's activities and objects
- Names of all trustees (or equivalent)
- Names or classes of beneficiaries

8.15 Church Bodies

Churches are in general exempted by law from registering as charities and will not therefore have a registered number.

The identity of a church body should be verified by:

a) Writing to the appropriate headquarters or regional organisation of the denomination; or
b) Obtaining sight of the General Register Office Certificate (GRO)
c) Verification of their status via HMRC

Additionally, at least two primary contacts should be verified as private individuals, with their capacity to act noted.

8.16 Local Authorities, Government Departments, Universities

When arranging transactions for the above the following checks will be undertaken:

a) The principal address of the body should be verified. This could be achieved via a visit to premises, by obtaining sight of documentation (e.g. utility bills sent to the organisation at the address) or by finding the organisation listed by an official source at the address in question;
b) Steps should be taken to confirm the legal standing of the organisation i.e. to confirm the organisation is indeed what it purports to be.
c) Verify that the individual with whom you are dealing has authority to act. This will usually be achieved through one of the following:
    - Calling the company on an independently verified number (e.g. from the phone book) and check the individuals credentials with a third party at the firm. Again it is likely that you would also need to inform the client that this was part of your procedure;
    - Obtaining confirmation from the legal department of the organisation that the individual is authorised to act.

NB – Before acting for organisations of this nature it is important to check that the organisation falls within REMITTVEN LTD's 'Scope of Permission' to act.

Many governmental, supranational and state-owned organisations will be managed and controlled by individuals who may qualify as PEPs. REMITTVEN LTD is aware of the increased likelihood of the existence of such individuals in the case of such customers, and deal with them appropriately, having regard to the risk that the funds of such entities may be used for improper purposes

8.17 Verification of Trusts

For trust cases the following verification checks will be carried out:

- The 'Settlor' must be verified as a private individual (or corporation as appropriate);
- The trustees must be verified as private individuals (or corporations as appropriate);
- Any controllers who have the power to remove trustees must be verified as private individuals (or corporations as appropriate);
- A certified copy of the trust deed must be obtained.

In respect of trusts, the firm will obtain the following information:

- Full name of the trust
- Nature, purpose and objects of the trust (e.g., discretionary, testamentary, bare)

- Country of establishment
- Names of all trustees
- Names of any beneficial owners
- Name and address of any protector or controller

Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

Beneficiaries

There is no requirement for advisers to verify the beneficiaries - the product provider will be required to carry out such checks at the point of payment of any benefits.

Source of Funds for Discretionary & Offshore Trusts

For discretionary and offshore trusts you must ascertain and record the nature and purpose of the trust and the original source of funding.

Where funds for an offshore trust are drawn from an account not under the control of the trustees, two authorised signatories on the account from which the funds are drawn must be verified as private individuals.

Life Policies in Trust

When term assurance contracts, with no investment element, are being placed in trust there is no requirement to verify the identity of the trustees at outset. In these circumstances only the identity of the premium payer needs to be verified (the plan has no value other than upon death – thus the trust only forms at this time). The life office will need to verify the identity of the trustees prior to releasing any funds in the event of a claim.

If a life policy is being placed in trust where the applicant is also a trustee, and where the trustees have no beneficial interest in the funds, you need only verify the identity of the person applying for the policy. The remainder of the trustees would, however, need to be identified where policy proceeds were to be paid to a third party not identified in the trust deed.

8.18 Powers Of Attorney and Third Party Mandates

Before acting for a client with a Power Of Attorney or third party mandate you should gain confirmation of the reasons for the granting of the Power Of Attorney/third party mandate.

Where third party mandates or Powers Of Attorney are in place you must obtain the following:

- Personal verification of the holder of the Power Of Attorney/third party mandate;
- Personal verification of the client themselves (i.e. the person upon whom the mandate or power of attorney is held);
- A certified copy of the Power Of Attorney or third party mandate.

Additionally anyone who inputs money or monies worth into the arrangement other than these parties – should also be verified.

8.19 Offshore Business Verification

Offshore Business

When conducting business offshore, money laundering verification requirements and the associated identification checks differ due to different legislation affecting offshore centres. *Please note that, if the client is situated in another territory, Firms need to check with the local financial services regulator whether or not they are deemed to be performing a regulated activity.*

Offshore centres such as the Isle of Man, the Channel Islands and Luxembourg exist and we recommend that you contact the product provider operating in the offshore centre itself who should be able to provide anti-money laundering procedural guidance for the specific offshore centre.

8.20 Verification of Identity for Lawyers, Accountants & Atypical Clients

Establishing identity for Lawyers and Accountants

Lawyers and Accountants, when acting in the course of their business as regulated firms or individuals, can be verified by reference to their Practising Certificates. Checks on their regulated status can be made through reference to the current membership directory of the relevant law society or accountancy body. However, when they are acting in their personal capacity, for example, as trustees or for their own investments etc, their identity should be verified as for any other individual.

When establishing the identity of solicitor or accountancy partnerships the rules in governing due diligence measures for private individuals should be followed.

Establishing identity for Children

The basic principles of identity verification apply i.e. that you verify the owner of the funds, the controller of the funds and the provider of the funds. For children, a family member or guardian will normally open and control the account. In these cases evidence of identity of the relevant adults should be obtained in the usual way. It is important to note that in many circumstances the person providing the funds might be different to the person who will be able to operate the account (e.g. where a grandparent is providing the funds for a policy in a child's name, it will be the parent or legal guardian who would be mandated to deal with those funds until the child came of age). Accordingly more than one adult might need to be verified.

As well as verifying the relevant adults, the child's identity should be evidenced by obtaining sight of their birth certificate (birth certificates are acceptable evidence for children only), passport or NHS Card. Their home address can be certified by obtaining evidence that the parents reside at the same address - (using the usual documentation).

Establishing identity for UK based students and minors

In most cases it should be possible to verify the personal identity of students and minors from the acceptable documents for verification as listed in section 6. For students studying away from home, further evidence of address may be obtained:

- From the home address of the parent / guardian;
- By obtaining confirmation of the UK address from the applicant's college or university, any confirmatory letter should be on appropriately headed notepaper;
- By seeking evidence of a tenancy agreement or student accommodation contract;

However, care should be taken at the commencement of the academic year before a student has taken up residence at the college / university, as registration frauds are known to occur at this time.

Establishing identity for prisoners and those on probation

In instances where the normal verification requirements cannot be achieved, a letter from a Prison Governor confirming the applicant is who they claim to be would be sufficient. If the applicant has been released, a letter from police or probation officer or hostel manager confirming identity would be sufficient.

Establishing identity for asylum seekers

Asylum seekers should have in their possession an 'Application Registration Card' (ARC). NB This document shows the status of the individual, and does not confirm their identity. This can be used in conjunction with other relevant documentation to help prove identification. However, care must be taken to ensure that the card hasn't been forged. If address verification cannot be verified via the relevant procedures then you may accept a letter from a responsible person in charge who can verify the address of the applicant. *For example, via a letter from a hostel or hotel manager confirming temporary residence.*

For those whose asylum claims have been accepted, blue United Nations Convention Travel Documents, brown certificates of identity issued by the Home Office or a letter from the Home Office confirming the applicant's refugee status are sufficient as evidence of name.

Establishing the identity for economic migrants
Economic migrants who are admitted into the UK with permission to work may prove their identity with a national passport or Identity Card (EEA and Switzerland issued). Alternatively they may use a GV3 Visa Form. This is a one-way photographic travel document issued by British Consulates around the world.

The Mentally Incapacitated
The affairs of people who are mentally incapacitated are generally handled in one of two ways. These are:

1) An Enduring Power Of Attorney is registered with the Court Of Protection. This gives the attorney power to manage their financial affairs. In all cases the Enduring Power Of Attorney document should carry the stamp of the Court Of Protection. In these cases you should verify the identity of the attorney and obtain sight of the stamped Power Of Attorney document.
2) A receiver may be appointed by the court to act on behalf of the mentally incapacitated person. In these cases the Public Guardianship Office advises the receiver to open an account in their name as receiver for the client. To do this they must be in receipt of either a 'Court Receivership Order' or a 'Short Order' from the court. In these instances the court documentation can be relied upon without obtaining further identification evidence.

8.21 Other regulated financial services firms that are subject to the ML Regulations (or Equivalent)

In respect of other financial services firms which are subject to the ML Regulations or equivalent, and which are regulated in the UK by the FCA, or in the EU or an equivalent jurisdiction, by an equivalent regulator, simplified due diligence may be applied. REMITTVEN LTD must have reasonable grounds for believing that the customer qualifies for the treatment. Having reasonable grounds might involve:

- checking with the home country central bank or relevant supervisory body; or
- checking with another office, subsidiary, branch or correspondent bank in the same country; or
- checking with a regulated correspondent bank of the overseas institution; or
- obtaining from the relevant institution evidence of its license or
- authorisation to conduct financial and/or banking business.

To assist firms, a list of the regulatory authorities in EU and FATF member states is available at www.jmlsg.org.uk. Firms should record the steps they have taken to check the status of the other regulated firm.

Firms should take appropriate steps to be reasonably satisfied that the person they are dealing with is properly authorised by the customer.

8.22 Other Firms that are subject to the ML Regulations

Customers which are subject to the ML Regulations or equivalent, but which are not regulated in the UK, the EU or an equivalent jurisdiction as a financial services business, should be treated, for AML/CTF purposes, according to their legal form: for example, as private companies, in accordance with the guidance set out in earlier sections. However, when professional individuals are acting in their personal capacity, for example, as trustees, their identity should normally be verified as for any other private individual.

REMITTVEN LTD must take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer Independent legal professionals that are subject to the ML Regulations, or from third countries where they are subject to equivalent requirements (and are supervised for compliance with those requirements), and which hold client money in pooled accounts, are obliged to verify the identities of their clients.

Financial services firms with which such client accounts are held are not required to identify the beneficial owners of such funds, provided that the information on the identity of the beneficial owner is available, on request, to the firm.

9. Politically Exposed Persons (PEP)

A PEP is defined as an individual who is or has been, at any time, been entrusted by a domestic and non-domestic power with prominent public functions or an immediate family member, or a known close associate, of such a person.

The following guidance is provided to clarify what is meant by the terms 'prominent public function', 'immediate family member' and 'close associate'.

People in Prominent Public Functions include:

- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of Parliament;
- Members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces; and (other than in respect of relevant positions at Community and international level);
- Members of the administrative, management or supervisory boards of State-owned enterprises.

These categories do not include middle-ranking or more junior officials exercising/discharging their duties at levels lower than national.

Immediate family members include:

- A spouse;
- A partner (including a person who is considered by their national law as equivalent to a spouse);
- Children of that person and their spouses or partners; and
- Parents of that person.

Under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Regulation 35(11) states that the provisions in Regulation 35(9) (that require a PEP to continue to be treated as a PEP after he or she leaves office) do not apply to family members who should be treated as ordinary customers, unless other risks are apparent, from the point that the PEP leaves office.

Close associates include:

- Any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP; and
- Any individual 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 a PEP.

<u>Identification of a PEP</u>

All new clients will be screened for matches against the RemitOne PEP databases.

<u>Acceptance of a PEP</u>

If identified, the decision on whether or not a firm can establish a business relationship with a PEP must be taken by the MLRO. If the MLRO provides approval, the firm will add the customer to the PEP Register and the MLRO will concurrently advise on the necessary enhanced due diligence and ongoing transactional monitoring measures required.

<u>Annual review</u>

REMITTVEN LTD will conduct an annual client review for all existing clients. As part of this review all clients will be asked to confirm if they meet the requirements to be defined as a politically exposed person or a connected person.

10. Non-Cooperative Countries

The FATF is the international body devoted to developing and promoting policies to combat money laundering and counter terrorist financing. As part of its work FATF maintains a list of non-cooperative countries.

Should you wish to transact business where the individual or the source of funds is from a non-cooperative country you must seek prior-approval and guidance from the MLRO.

11. Financial Sanctions

Financial sanctions can be administered against individuals, countries or regimes by the United Nations, European Union etc. Financial Sanctions can also be issued by individual countries: the United Kingdom, the United States of America etc.

UK legislation prohibits a firm from providing services to an individual or entity listed by these bodies as a target of financial sanctions. It also imposes notification requirements on firms that have any dealings with these individuals and/or entities.

For each new client, REMITTVEN LTD will check for any matches against the HMT Sanctions List using GBGID3 Global., This process will thereby be conducted on a yearly basis for all existing clients to comply with any necessary legal and regulatory requirements.

The HMT sanctions list can be found via the link below:

http://www.hm-treasury.gov.uk/fin_sanctions_index.htm

In addition, REMITTVEN LTD will also match all new and existing clients against international sanctions lists, including the US sanctions list using GBG ID3 Global.

If any clients are found to be a confirmed 'hit' on the Sanctions List, we must report that individual to the MLRO who will, if confirmed, report them to the Asset Freezing Unit of HM Treasury. The submission of a SAR report to the National Crime Agency by the Nominated Officer using SAR Online is also likely to be required.

Enquiries relating to asset freezing or other financial sanctions should be submitted to HM Treasury either by email to financialsanctions@hmtreasury.gsi.gov.uk or by post to:

Financial Sanctions

HM Treasury

1 Horse Guards Road

London

SW1A 2HQ

REMITTVEN LTD is also signed up to the HM Treasury's email alerts for information on updates relating to financial sanctions in effect in the UK.

12. Terrorist Lists

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

The sites below confirm lists of international terrorists:

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

It is an offence to provide financial services to any suspects / known terrorists.

Please ensure that you make proper due diligence checks of these lists particularly if you are dealing with individuals who are non-UK nationals or residents. Additionally, you must seek approval from the MLRO prior to conducting business with countries exposed to terrorism (e.g. but not limited to Iraq, Tunisia, Algeria, Syria and Yemen).

The Financial Action Task Force (FATF) publishes documentation available from its website which identifies those jurisdictions whose anti-money laundering and combating the financing of terrorism (AML/CFT) regimes it considers to be strategically deficient. The most recent of these documents (from 2017 confirmed that such countries included:

- Iran
- Democratic People's Republic of Korea (North Korea)
- Ethiopia
- Iraq
- Serbia
- Sri Lanka
- Syria
- Trinidad and Tobago
- Tunisia
- Vanuatu
- Yemen

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

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

13. Staff Awareness and Training

All relevant employees will be made aware of the risks of money laundering and terrorist financing, the relevant legislation and their obligations under the legislation.

All relevant employees will be made aware of the identity of the MLRO and its responsibilities.

All relevant staff will be trained in the firm's procedures and in how to recognise and deal with potential money laundering or terrorists financing transactions and activities.

REMITTVEN LTD will take reasonable steps to ensure that relevant employees are made aware of their responsibilities under the firm's arrangements for the prevention of money laundering and terrorist financing, including the requirements for obtaining sufficient evidence of identity, recognising and reporting knowledge or suspicion of money laundering or terrorist financing.

Staff training will be given at regular intervals and details recorded. The MLRO is responsible for the firm's internal compliance in respect of staff training. The MLRO also has overall responsibility for the establishment and maintenance of effective training arrangements.

14. Record Keeping Requirements

REMITTVEN LTD is subject to record keeping requirements under the Data Protection Act 1998, Money Laundering Regulations 19 and 20, and SYSC within the FCA handbook. Under these provisions, firms are obligated to keep:

- copies of, or references to, the evidence they obtain of a customer's identity for five years after the end of the customer relationship;
- details of customer transactions for five years from the date of the of the transaction
- details of actions taken in respect of internal and external suspicion reports for a period of five years from date of construction
- details of information considered by the nominated officer in respect of an internal report where no external report is made for a period of five years from date of construction
- MLRO annual (and other) reports

The objective or aim of record keeping is to maintain an audit trail to help the MLRO and the authorities investigate any allegation of money laundering, in order to assist in any financial investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

14.1 Data Retention

REMITTVEN LTD may wish, or find it necessary, to rationalise their hard copy filing requirements, when seeking to reduce the volume and density of records which have to be stored, therefore retention may be by way of:

- Original hard copy documents;
- Photocopies of original documents;
- Microfiche;
- In scanned form;
- Computerised or electronic files.

All statutory requirements apply regardless of how records are stored.

Record retention requirements are the same regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means.

Relevant records relating to the verification of identity should be stored securely. It must be possible for relevant information to be retrievable within 24 hours.

If there is an ongoing investigation into a file then the firm will retain all relevant documentation until the case has been closed by the MLRO or the relevant law enforcement agency.

14.2 Sanctions and Penalties

Where the record keeping obligations under the ML Regulations are not observed, REMITTVEN LTD is open to prosecution, including imprisonment for up to two years and/or a fine.