Financial crime policy and procedure

Table of Contents

Document Control

Approver(s)	Board of Directors
Policy Owner	MLRO – Alexander Kostiaev
Version	1.0
Status	Operational
Last Reviewed Date	June 2020
Date of Next Scheduled Review	June 2021

Background documents reference

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('The Money Laundering Regulations 2017')
- Proceeds of Crime Act 2002 (as amended) ('POCA')
- The Criminal Finances Act 2017
- Terrorism Act 2000, and the Anti-terrorism, Crime and Security Act 2001
- Counter-Terrorism Act 2008, Schedule 7
- Financial sanctions guidance published by HM Treasury
- Guidance issued by the Joint Money Laundering Steering Group ('JMLSG') on 'Prevention of money laundering/combating terrorist/financing'
- FCA Financial Crime Guide for Firms
- The Bribery Act 2010
- The Fraud Act 2006

1. Introduction

1.1 Guidance

The primary purpose of this Financial Crime Guidance (the 'Guidance') is to document the approved Policy and guidance of PAYPORT UK relating to:

- Financial crime – Preventing PAYPORT UK's association with money laundering, terrorist financing, fraud, and bribery & corruption
- Establishing new customer relationships

and

- Monitoring of existing customer relationships

In addition, the Guidance:

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

1.2 Financial crime policy statement

PAYPORT UK is responsible for assessing money-laundering risk and ensuring appropriate implementation of risk-sensitive policy and procedure within the business. The company fully supports the UK's AML regime and has zero tolerance for criminal use, or misuse, of PAYPORT UK's services in furtherance of money laundering.

PAYPORT UK is committed to ensuring that:

- the risk of PAYPORT UK being used as a vehicle for money laundering or terrorist financing is minimised
- appropriate knowledge and awareness are maintained in the business, of the UK's AML requirements and relevant law
- PAYPORT UK complies with regulatory requirements of the Financial Conduct Authority ('FCA') to prevent and forestall use of PAYPORT UK by criminals to carry out financial crime
- where transactions suspected to involve money, laundering are recognised, these will be reported to the appropriate authorities, including any linked to persons or entities suspected of being involved in or supporting acts of terrorism
- should a customer of PAYPORT UK come under investigation by law enforcement, PAYPORT UK will be able to provide its part of any relevant audit trail, in respect of transactions or information about the customer, held by PAYPORT UK

PAYPORT UK expects its employees to:

- Comply with PAYPORT UK's Financial Crime Policy Statement ('the Policy')
- Attend Know Your Customer ('KYC') and AML training within 15 days of beginning employment
- Be alert to money laundering, fraud and other forms of financial crime, including bribery & corruption, and financial sanctions risk; and to report incident or suspicion to management (as per this Guidance)
- Ensure timely reports of all money laundering suspicions identified in any transaction/arrangement associated with PAYPORT UK business

1.3 The Business

Licensing

The FCA is the competent authority under the Electronic Money Regulations and Payment Services Regulations to authorise/register payment institutions and to enforce compliance by payment service providers, with applicable conduct of business requirements

The Money Laundering Regulations 2017, give the FCA responsibility (HMRC for firms who have Money Remittance Permission only) for supervising the anti-money laundering controls of businesses that provide payment services.

1.4 Core regulatory requirements

As a provider of payment services for customers, PAYPORT UK is required, to:

1. Appoint a Nominated Officer/ Money Laundering Reporting Officer
2. Ensure that documentation carries specified information about the Payer who gives instruction for a payment to be made
3. Assess money laundering risk associated with PAYPORT UK's customers
4. Implement risk-sensitive procedure, which serve to reduce the risk of the business being used by money launderers and terrorists, including procedure linked to:
    - Customer take-on
    - Account monitoring arrangements
    - Record retention procedure
5. Provide relevant training to management and employees
6. Report suspicions of money laundering to the UK's National Crime Agency ('NCA')

1.5 Senior management responsibility

Policy implementation and review

Alexander Kostiaev is the senior manager responsible for ensuring that PAYPORT UK adheres to the Money Laundering Regulations 2017.

PAYPORT UK's senior management will adhere to the following guiding principles:

- An unequivocal commitment to ensuring a compliant culture and values to be adopted and promulgated throughout the firm towards the prevention of financial crime
- A commitment to appointing a Money Laundering Reporting Officer/Nominated Officer which will manage the financial crime framework
- A commitment to ensuring that customers' identities will be satisfactorily verified before the firm accepts them
- A commitment to the firm 'knowing its customers' appropriately - both at acceptance and throughout the business relationship - through taking appropriate steps to verify the customer's identity and business, and his reasons for seeking the particular business relationship with the firm
- A commitment to ensuring that staff are trained and made aware of the law and their obligations under it, and to establishing procedures to implement these requirements; and o recognition of the importance of staff promptly reporting their suspicions internally

1.6 Money Laundering Reporting Officer/Nominated Officer responsibility

The MLRO/NO is responsible for the following:

- Oversight of PAYPORT UK's compliance with its requirements in respect of MLR2017
- Determining whether to approve the take-on (or retention) of customers identified as Politically Exposed Persons; and the steps to implement should monitoring be required of such a relationship
- Appropriate record keeping on:
    - Policy compliance and assurance arrangements
    - Effectiveness of AML compliance arrangements
    - Recommendations or enhancements required in PAYPORT UK's financial crime arrangements, to mitigate identified new/emerging risk
- Ensure that client data is deleted as following:
    - Any personal data is deleted after 5 years from the end of business relationship
    - All data is deleted after 10 years from the end of business relationship

- Guardian of PAYPORT UK's compliance with UK Bribery & Corruption legislation
- Person to whom reports of suspected fraud, financial sanction risk or other irregularity are to be reported
- The person responsible for determining whether internal reports of money laundering suspicion should be disclosed to the National Crime Agency ('NCA')
- The person responsible for liaison with law enforcement authorities

1.6 Employee responsibility

All employees of PAYPORT UK are expected to adhere to the values of the firm's financial crime prevention framework, attend all training, understand the procedures involved and report any suspicious activity.

2. Money laundering and Terrorist Financing

2.1 What is money laundering?

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

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

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

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

2.2 Money Laundering Offences

The Proceeds of Crime Act ('POCA') includes various criminal offences related to money laundering. A person may commit a money laundering offence[1] if he:

- Conceals, disguises, converts or transfers criminal property, or removes criminal property from England and Wales, or

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

from Scotland or from Northern Ireland (s327)
- Enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person (s328)
- Acquires, uses or has possession of criminal property except where adequate consideration was given for the property (s329)

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

But under POCA an offence may not be committed where:

- Persons did not know or suspect that they were dealing with criminal property
- A report of an identified suspicion is made promptly to: the person responsible for money laundering, the Nominated Senior Person or the firm's MLRO (money laundering reporting officer), or to a person authorised to receive SARs by the NCA (National Crime Agency), (if the report is made before the act is committed) the appropriate consent is obtained before doing the act
- No report is made, with a reasonable excuse for the failure (e.g. under duress, threat or intimidation - might be acceptable reasons)
- Conduct giving rise to the criminal property was reasonably believed to have taken place outside of the UK, and the conduct was in fact lawful under the criminal law of the place where it occurred, and the maximum sentence if the conduct had occurred in the UK would have been less than 12 months

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

2.3 What is Terrorist Financing?

The Terrorism Act 2000 (as amended by the Terrorism Act Amendment Regulations 2007) has established several offences relating to handling or possessing funds or other property to be used for terrorist purposes. The definition of 'terrorist property' means that all dealings with funds or property (which are likely to be used for the purposes of terrorism), even if the funds are "clean" in origin, is a terrorist financing offence.

A person may commit Terrorist Financing if they are involved in the following:

- Fund raising, which covers inviting other people to provide money or other proceeds to support terrorism
- Use and possession, which covers using money or other proceeds for the purpose of terrorism
- Funding arrangements, if a person knowingly enters into an arrangement whereby they provide funding for terrorists

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

When dealing with customers you need to be aware of the threat of terrorist financing.

2.4 Identifying Terrorist Financing

There can be considerable similarities between Terrorist Financing and Money Laundering. However, there are two major differences between them.

- Terrorist Financing often involves small amounts at a time making it harder to spot. Whereas Money Launderers can launder thousands at a time, terrorist financing can be in the hundreds
- Terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist proceeds

2.5 Failing to Disclose

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

Similar provisions regarding failure to disclose are contained in s19, and 21A, Terrorism Act 2000. s21A is applicable to all those in the regulated sector.

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

The obligation to make the required disclosure arises when:

- A person knows or suspects, or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering
- The information or other matter on which a suspicion is based came to him in the course of business in the regulated sector
- He either can identify that other person, or has information concerning the whereabouts of the laundered property or the information he has may assist in identifying the person or the whereabouts of the property (the laundered property is that which forms the subject matter of the known or suspected money laundering).
- When submitting an internal report to the MLRO/ Nominated Senior Person:
- MLROs/ Nominated Senior Person have a duty to make disclosures under POCA or the Terrorism Act 2000, if they have knowledge, suspicion or reasonable grounds to suspect money laundering or terrorist financing, as a consequence of an internal report
- An MLRO/ Nominated Senior Person may commit an offence if he fails to pass on reportable information in internal reports that he has received, as soon as is practicable, to NCA

2.6 Tipping-Off

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

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

A tipping-off offence may not be committed if: the person did not know or suspect that the disclosure was likely to prejudice any investigation that followed, the disclosure is made to the FCA or other relevant supervisor for the purpose of: detection, investigation or prosecution of criminal offences under the law, investigation under POCA or the enforcement of any order of a court under POCA. Furthermore, an offence would not be committed if the disclosure is to an employee, officer or partner of the same firm. Nor is an offence committed if the firm is making a disclosure, and the firm to which it is made belongs to the same group and: the disclosure is to a credit institution/financial institution and the firm to which the disclosure is made is situated within an EEA state.

The penalty for a tipping off offence under POCA, on conviction on indictment, is imprisonment for a term not exceeding two years, or a fine or both. The Terrorism Act 2000 has a similar tipping-off offence in relation to prejudicing terrorism investigations.

3. What are the Money Laundering and Terrorist Financing Risks?

There are several features of the Payments Industry that can make it susceptible to Money Laundering and Terrorist Financing. Transactions can be simple, and they can have a global reach. They can often be low threshold transactions with less stringent customer due diligent rules compared with banks and other financial institutions. The infrequent contact that customers also have with Payment Service Providers may also increase the risk. In addition to this, there are occasions when cash transactions can be involved which will increase the risk.

The main ways in which a Payment Service Provider can be used for Money Laundering or Terrorist Financing are:

- Either knowingly or unknowingly performing relevant transactions for their customers without knowledge of the illegal origin or destination of the funds concerned
- Direct involvement of the staff/management of the Payment Service Provider through complicity or through the ownership of such businesses by a criminal organisation

Payment Service Providers can be used at all stages of the Money Laundering Process. Currency exchanges specifically are an important link in the money laundering chain. Once the money has been exchanged, it is difficult to trace its origin.

The above risks can be mitigated by ensuring that Due Diligence and Monitoring measures are applied, and reporting obligations are adhered to.

4. Who is the Customer for AML & CTF Purposes?

The typical customers to whom services will be provided include private individuals, sole traders, partnerships and unincorporated bodies of persons. In addition to this some larger Payment Service Providers will provide services to corporate clients. In such cases the firm's customer will be the individual or entity concerned. The firm must also consider whether there are any beneficial owners or controller.

5. Requirements under the Wire Transfer Regulations

5.1 Information requirements

New Wire Transfer Regulations require information on the payer and payee and the level of detail will depend on whether the transfer is from within or outside the EU:

Transfer Location	Payer Information Needed	Payee Information Needed
Outside the EU	▪ Name ▪ Account number or transaction ID ▪ Address ▪ If need be the address can be substituted by date and place of birth, customer ID number and national ID number	▪ Name ▪ Account number or transaction ID
From within the EU	Account number or transaction ID	Account number or transaction ID

5.2 Verification Rules

Sending funds on behalf of the payer – when the payment totals more than €1,000 you will need to verify the identity and address (or alternative used) of the payer.

Receiving funds on behalf of the payee – when you are receiving a payment of more than €1,000 for a customer you will need to verify the accuracy of the information included and report any discrepancies.

6. Risk management and Controls

6.1 Client Due Diligence

PAYPORT UK's client due diligence consists of the following:

- Identifying the client and verifying the client's identity using documents or information from a reliable and independent source
- Identifying the beneficial owner and verifying that person's identity, taking measures to understand the ownership and control structure of the client, where applicable
- Assessing the purpose and intended nature of the business relationship (business profile)

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

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

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

PAYPORT UK has decided as a business that Simplified Due Diligence will not be performed on any clients and either Normal Due Diligence or Enhanced Due Diligence will be performed.

Private individuals

Identifying private individuals as clients

PAYPORT UK will obtain the following information for prospective clients that are individuals:

- **Full name**
- **Residential address**
- **Date of birth**

Verifying identities of private individuals

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

Documentary evidence should include government issued documents with photos, such as valid passport, photo card driving license or national identity card, or government issued documents without photos which incorporate the client's full name

and either his residential address or his date of birth, supported by a second document either government issued, issued by a judicial authority, a public sector body, a regulated utility company or another FCA regulated firm in the UK.

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

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

- Requiring the first payment to be carried out through an account in the client's name with a UK or EU regulated credit institution
- Telephone contact with the client on a home or business number that has been verified, prior to opening the account
- Communicating with the client at the address that has been verified
- Requiring copy documents to be certified by an appropriate person

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

Corporate clients

Identifying corporate clients

PAYPORT UK will obtain the following information for prospective clients that are corporates:

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

And for private or unlisted companies:

- **Names of all the directors**
- **Names of individuals who own or control over 25% of its shares or voting rights**
- **Names of any individuals who exercise control over the management of the company**

Verifying identities of corporate clients

PAYPORT UK will verify the identity of the client by confirming the company's listing on a regulated market, searching the relevant company registry or viewing a copy of the company's Certificate of Incorporation.

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

Unincorporated clients

Identifying unincorporated clients

PAYPORT UK will obtain the following information for prospective clients that are unincorporated:

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

Verifying identities of unincorporated clients

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

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

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

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

PAYPORT UK will obtain the following information for prospective clients that are public sector bodies, governments, state owned companies or supranationals:

- **Full name of entity**
- **Nature and status of entity**
- **Address of the entity**
- **Name of the home state authority**
- **Names of directors**

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

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

Pension scheme clients

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

Charity, church body, trust and foundation clients

Identifying charity, church body, trust and foundation clients

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

- **Full name and address**
- **Nature of activities and objects**
- **Names of all trustees**
- **Names or classes of beneficiaries**
- **Country of establishment (for trusts and foundations)**
- **Name and address of any protector or controller (for trusts and foundations)**

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

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

PAYPORT UK will also verify the identities of the trustees.

Politically Exposed Persons (PEP)

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

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

PAYPORT UK will check all clients at initial account set up and on annual basis to identify any PEPs, using Credit Safe or another source. If a PEP is identified, the MLRO will be notified and enhanced due diligence measures will be employed.

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

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

Once due diligence is complete, approval will be sought from the MLRO prior to completion of account set up or any transactions being carried out.

Where approval is granted to continue with the PEP relationship the reasoning will be documented by the MLRO and the nature and extent of the on-going monitoring of the account will be agreed with the relevant teams in PAYPORT UK.

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

6.2 Customer Risk Assessment

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

The client risk assessment will also take into account customer risk factors, product, service, transaction or delivery channel risk factors and geographical risk factors.

Low Customer risk factors:

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

High Risk Customer risk factors:

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

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

a) life insurance policies for which the premium is low
b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral
c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme

d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes
e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money)

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

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

Low Geographical risk factors:

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

High Geographical risk factors:

a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective Anti-Money Laundering systems
b) countries identified by credible sources as having significant levels of corruption or other criminal activity
c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations
d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country

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

6.3 Enhanced Due Diligence (EDD)

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

PAYPORT UK's enhance due diligence measures include:

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

a) About the client's or beneficial owner's identity, or ownership and control structure, to be satisfied that the risk associated with the relationship is well known. This may include obtaining and assessing information about the client's or beneficial owner's reputation and assessing any negative allegations against the client or beneficial owner. Examples include: information about family members and close business partners; information about the client's or beneficial owner's past and present business activities; and adverse media searches

b) About the intended nature of the business relationship, to ascertain that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete client risk profile. It includes obtaining information on:

- the number, size and frequency of transactions that are likely to pass through the account to be able to spot deviations that may give rise to suspicions, requesting evidence where appropriate
- the reason the client is looking for a specific product or service, in particular where it is unclear why the client's needs cannot be met better in another way, or in a different jurisdiction
- the destination of funds
- the nature of the client's or beneficial owner's business to understand the likely nature of the business relationship better

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

a) Requiring the first payment to be carried out through an account verifiably in the client´s name with a bank subject to UK Client Due Diligence standards

b) Establishing that the client's source of wealth and source of funds that are used in the business relationship are not the proceeds from criminal activity and that they are consistent with PAYPORT UK's knowledge of the client and the nature of the business relationship. The sources of funds or wealth may be verified, among others, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent and credible media reports

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

- Increasing the frequency of reviews of the business relationship, to ascertain whether the client's risk profile has changed and whether the risk remains manageable
- Obtaining the approval of the MLRO to commence or continue the business relationship to ensure senior management are aware of the risk PAYPORT UK is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk
- Reviewing the business relationship on a more regular basis to ensure any changes to the client's risk profile are identified, assessed and, where necessary, acted upon

- Conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that may give rise to suspicion of money laundering or terrorist financing. This may include establishing the destination of funds or ascertaining the reason for certain transactions
- The MLRO will need to provide approval, or refusal, to proceed with the client set up process prior to conducting any business with a client who has been through the enhanced due diligence process

6.4 Financial Sanctions

PAYPORT UK will review all clients to ensure that they are not on the Financial Sanctions register as published by HM Treasury, at initial client set up and then on an annual basis. PAYPORT UK will not set up accounts for clients on the Financial Sanctions Register or carry out any transactions with them.

It is a criminal offence to make funds or Financial services available to individuals or entities on the sanctions list. The latest list can be found here:

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

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

Employees will discuss any clients that appear on the sanctions list with the MLRO in the first instance. If a prospective client is on the sanctions list, then PAYPORT UK will start an official investigation to determine the exact nature of the sanction. PayPort UK will also halt further account set up and report the matter to the Office of Financial Sanctions at the HM Treasury – contact details as follows:

Office of Financial Sanctions Implementation
HM Treasury 1 Horse Guards Road London SW1A 2HQ
TEL. 020 7270 5454 or
email ofsi@hmtreaury.gsi.gov.uk

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

6.5 Ongoing Monitoring

PAYPORT UK will continually monitor its clients for signs of money laundering, focusing on transaction monitoring and client reviews.

Transaction monitoring

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

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

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

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

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

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

- Establishing the source and destination of the funds
- Finding out more about the client's business to understand the rationale for the transactions
- Monitoring the business relationship and subsequent transactions more frequently

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

Client reviews

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

PAYPORT UK has a customer review process based on the High, Medium and Low risk factors assigned to its customers.

Re-verification of identification

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

High Risk Clients

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

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

Medium Risk Clients

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

- Re-confirmation of Address
- Re-confirmation of Corporate Structure (if applicable)
- Screening for adverse news
- Complete review of transaction profile, including new products requested

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

Low Risk Clients

Low risk customers will be reviewed on a risk-based approach. Reviews will be undertaken when trigger events occur such as:

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

This review will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Corporate Structure (if applicable)
- Screening for adverse news

- Complete review of transaction profile, including new products requested

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

Trigger events

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

MLRO/Nominated Officer reviews

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

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

6.6 Reporting Suspicious Transactions

Employees are expected to be alert to money laundering and they are responsible for reporting any actual or suspected money laundering to the MLRO in a timely manner.

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

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

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

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

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

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

Subsequent investigations

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

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

6.10 Politically Exposed Persons

A PEP is defined as "an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person". Historically this only applied to those holding such a position in a state outside the UK, however the EU Fourth Money Laundering Directive is set to change that with the definition being widened to cover both domestic and foreign PEPs.

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

Where as a result of information identified via World-Check or another source, information suggests that an applicant, existing customer, or a beneficiary is a PEP, this should immediately be reported to the MLRO (in the case of full permission lenders) or Nominated Senior Person (in the case of all other firms) for EDD purposes:

- The MLRO/ Nominated Senior Person will cause any necessary additional due diligence to be conducted, in order to:
  - Assess the money laundering risk
  - Determine whether it is appropriate to continue with the PEP relationship

The assessment will include scrutiny of the relevant person's personal circumstances or change in status, as well as any identifiable complexity or structuring of the business relationship (e.g. involving companies, trusts or foreign jurisdictions), to ensure clarity about and legitimacy of any transaction(s).

Although, by definition, an individual might cease to be a PEP after having left office for one year, a risk-based assessment is still required when determining whether appropriate monitoring of transactions or activity should continue to be applied at the end of this period. A longer period might be appropriate in order to ensure that the higher risks associated with an individual's previous position have adequately abated.

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

- Approval should be obtained from the MLRO (or other senior manager) or Nominated Senior Person to establish (or continue) a customer relationship with a newly identified PEP

- Adequate steps should to taken establish the source of wealth and source of funding to be involved in the customer relationship or transaction
- The MLRO/Nominated Senior Person should ensure appropriate planning for conducting enhanced on-going monitoring if such a higher risk customer relationship is entered into or continued

Where, a decision is made to continue with a PEP relationship the reasoning must be documented by the MLRO or the Nominated Senior Person who should liaise with the business, to establish the:

- Nature and extent of information and on-going monitoring that should be captured and applied to the customer relationship

  and

- Duration and frequency of monitoring required

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

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

7. Identification Requirements –New Applicants

7.1 Private individuals

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

- **Full name**
- **Current residential address**
- **Date of birth**

Where electronic verification is not appropriate, evidence to verify identity can take a number of forms. For a private individual reliance is often placed on an identity document, such as, a passport or photo-card driving licence:

- Being documents issued by a government agency these are often the easiest way of being reasonably satisfied as to someone's identity
- But, sole reliance on such a document reflects an underlying assumption that everyone has either a passport or a driving licence

- It is possible to be reasonably satisfied as to an applicant's identity based on other reliable forms of confirmation, including, were appropriate, certain documents without photographs and written assurances from persons or organisations that have dealt with an applicant for some time

To verify a private individual's identity or determine whether he/she is a PEP, subject of a Financial Sanction, or a potentially higher risk customer for other reasons, information disclosed on the customer application form might be used, together with data or other information obtained from reliable and independent sources.

Other information/data might include details about:

- Marital status/family circumstances
- Previous home address
- Nature and place of employment/business career
- Contact with public authorities
- Contact with financial sector firms
- Physical appearance
- Details of property ownership
- Details of historic employment
- Membership of professional bodies, accredited organisations, etc.

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

Either

a government-issued[2] document which incorporates:

- the customer's full name and photograph

and

- either his residential address
- or his date of birth

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

or

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

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

The section below headed 'Identification Documents' identifies typical documentary evidence that is considered acceptable when seeking to confirm identity of a UK/EU resident. In normal circumstances, the applicant should be asked to supply two items of identity verification (i.e. one from List A and one item from List B on page 34), in some instances originals may be required, but on a risk based approach, it may be appropriate to accept copy documents supplied which are endorsed by an Appropriate Person.

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

Notes:

- At least one item must include a signature
- Documents from the same source cannot be used twice
- Photocopies when required, e.g. in certification process, should be **black and white** and unaltered

For PEPs and other higher-risk situations, where EDD is to be applied, PAYPORT UK should determine what additional information must be obtained, or higher level of verification completed.

7.2 Private (or unlisted) company

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

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

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

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

For company applicants, PAYPORT UK must:

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

Standard Evidence

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

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

Plus:

Either

A private company does not usually qualify for SDD. Under a risk-based approach, however, provided that confirmation is provided in writing by a reliable and independent source, the imposition of, say, regulatory obligations on an applicant firm (or customer) which is a private company, might be considered to provide an equivalent level of confidence in the company's public accountability.

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

Or

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

- The company's existence should be verified from:
  - either confirmation of the company's listing on a regulated market
  - or a search of the relevant company registry
  - or a copy of the company's Certificate of Incorporation
- The following information must also be obtained:
  - Names of all directors

- Names of beneficial owners who hold or control over 25% of the shares or voting rights or otherwise exercise control over the management of the company

Where electronic verification is not possible (for either corporate or personal identity verification) and reliance is to be placed on documentation supplied by an:

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

Directors

Following assessment of the money laundering or terrorist financing risk presented by a customer company, it may be appropriate to verify the identity of one or more directors, as appropriate, in accordance with the principles for private individuals (i.e. see 7.1 above).

In that event:

- Verification is likely to be appropriate for those who have authority to operate an account or to give PAYPORT UK instructions concerning the use or transfer of funds, but might be waived for other directors
- A requirement may already exist to identify director(s) as beneficial owner(s) if they own or control more than 25% of the company's shares or voting rights

Beneficial owners

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

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

or

- In respect of any body corporate, otherwise exercises control over the management of the body

As part of collecting standard evidence, PAYPORT UK is responsible for requesting from applicants details of beneficial ownership, of all individual beneficial owners owning or controlling more than 25% of the applicant company's shares or voting rights, even where these interests are held indirectly.

Verification requirements differ between a customer and a beneficial owner:

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

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

Mandate signatories

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

Where the identity of relevant company directors has been verified, the identities of individual signatories need only be verified on a risk-based approach. If, for example, all payment instructions are expected to originate from a customer's in-house accountant, who is not the Finance Director, a risk-based approach might be to verify the Accountant's identity.

PAYPORT UK is responsible for ensuring, that:

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

7.3 Companies listed on regulated markets

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

This is due to the fact that such companies are publicly owned and generally accountable. The exemption also applies to companies that are majority-owned and consolidated subsidiaries of such companies.

If a regulated market is located within the EEA there is no requirement to undertake checks on the market itself. Sales should, however, record the steps they have taken to ascertain the status of the market.

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

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

The European Commission maintains a list of regulated markets within the EU at https://ec.europa.eu/info/node/7511

7.4 Other customer types

The majority of PAYPORT UK customers are expected to be corporate operating within the UK and EU. Instances may arise however, when other customer types may be encountered. This section of Guidance provides an overview of the main other types of customer which might be encountered and their respective identification requirements.

7.5 Trusts

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

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

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

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

The trustees of a trust will be beneficial owners, as they will exercise control over the trust property. In exceptional cases, another individual may exercise control, such as a trust protector, or a settlor who retains significant powers over the trust property.

For the vast majority of trusts, either there will be clearly identified beneficiaries (who are beneficial owners within the meaning of the MLR), or a class of beneficiaries. These persons will be self-evident from a review of the trust's constitution.

In the case of a legal arrangement that is not a trust, the beneficial owner means

- where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25% of the property of the entity or arrangement
- where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interest the entity or arrangement is set up or operates
- any individual who exercise control over at least 25% of the property of the entity or arrangement

Details to be recorded and maintained:	Obtain the following: ▪ Full name of Trust ▪ Nature and purpose of Trust (e.g. discretionary, testamentary, bare) ▪ Country of establishment ▪ Names of all trustees ▪ Names of any beneficial owners ▪ Name and address of any protector or controller
Documentary evidence required to verify legal purpose:	Scheme Trust Deed or latest Deed of Appointment, listing all current Trustees

Additional:	▪ Names, addresses and dates of birth and identity verification required for trustees in whose names an investment is registered (i.e. if trustee is a private individual, personal identity and address verification also required) ▪ Names and confirmation of the identity of any other trustees, names and addresses and confirmation of the identity of any protector or controller, plus names and confirmation of identity of any nominated beneficiaries having an interest of at least 25% ▪ Identification for any third-party payers

7.6 Partnership/unincorporated body

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

The beneficial owner of a partnership is any individual who ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership, or more than 25% of the voting rights in the partnership, or who otherwise exercise control over the management of the partnership.

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

Where numbers are larger, decide whether to regard the customer as a collection of private individuals, or whether it might be appropriate to be satisfied with evidence of membership of a relevant professional or trade association. In either circumstance, there is likely to be a need to see the partnership deed (or other evidence in the case of sole traders or other unincorporated businesses), to be satisfied that the entity exists, unless an entry in an appropriate national register may be checked.

Details to be recorded and maintained:	Obtain the following: ▪ Business address ▪ Names of all partners/principals who exercise control over the management of the partnership ▪ Names of individuals who own or control over 25% of its capital or profit, or of its voting rights ▪ 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
Documentary evidence required to verify legal purpose:	Partnership deed showing rights and duties of the partners
Additional:	Name, address, date of birth and identity verification is required for partners or owners in whose names investments are registered (i.e. for private individuals, personal identity and address verification is required)

7.7 Charities	
Details to be recorded and maintained:	Obtain the following: ▪ Nature of body's activities and objects ▪ Names of all trustees (or equivalent) ▪ Names or classes of beneficiaries
Documentary evidence required to verify legal purpose:	Charities have their status because of their purposes, and can take a number of legal forms. Some may be companies limited by guarantee, or incorporated by Royal Charter or by Act of Parliament; some may take the form of trusts; others may be unincorporated associations Names, addresses, dates of birth and identity verification required for the trustees/officers in whose names investments are registered. Trustees/Officers should have appropriate authority to operate an account or give instructions to Pearl concerning the use or transfer of funds or assets (for private individuals, personal identity and address verification is required)
Additional:	Confirmation of the identity of all other officers/trustees (i.e. Name, address and dates of birth); this can be achieved by one of the verified partners or proprietors providing an original signed letter on the customer's letterhead, incorporating a listing of relevant persons (i.e. other officers)

8. Identification Documentation

8.1 Verifying identity using documentation

In circumstances where on-line verification of client identity is not possible, the minimum standard of documentary identity verification required, is:

One item from List A plus one item from List B (see below) - One of which must include a signature and one of which must include a photograph of the client

Notes:

1. The same document cannot be used as an option to fulfil requirements of both lists
2. Where a client submits an original document, care should be taken to make a clear legible office copy, after which the original should be returned to the client in the same class of mail used for delivery. Office copies should be retained with client records - after being endorsed on the rear (by PAYPORT UK who made the copy), with:
    a. 'Original seen on dd/mm/yyyy'

and

b. The employee's signature

3. Where a client provides copy documents in support of his/her identity, these:
    a. Should be black and white and unaltered
    b. Must be clear and legible copies of pages which provide/include a client's photograph, personal identity details, any government or government agency issued personal reference/account identifiers issued in the client's name

4. A copy of a document provided by a client to be used to verify identity, may be acceptable where:
    a. Instead of PAYPORT UK certification being applied (as per 2 above) and except where concern or doubt exists about authenticity of a document, the signature of an appropriate person certifying a copy document, may be acceptable
    b. Copy documents certified by an appropriate person must be:
        i. Endorsed as being copies of originals the signatory has seen
        ii. Certified by someone independent of the client, who:
            - Is not a relative
            - Holds a responsible position in society
            - Provides a UK contact telephone number (not a mobile number)

and

EITHER

- Where the Guidance on 'acceptable signatories' has been adopted

OR

- PAYPORT UK otherwise validates authenticity of copy documents; *and* Evidence of validation is retained with, or its location is cross-referenced to the relevant client records

LIST A

- Unexpired passport
- Unexpired UK old style driving licence (not provisional)
- Unexpired UK photo card driving licence
- EEA or Switzerland national identity card
- Firearms certificate or shotgun licence issued by a Police authority
- Northern Ireland voters card
- Council tax bill / demand letter *
- Notification of entitlement to state / local authority benefit *

- Notification of entitlement to tax credit *
- Notification of entitlement to pension from the DWP *
- Notification of entitlement to educational loan / grant *
- Notification of entitlement to other government / local authority grant *
- HMRC (Inland Revenue) coding / assessment / statement / tax credit *

LIST B

- Unexpired passport
- Unexpired UK old style driving licence (not provisional)
- Unexpired UK photo card driving licence
- EEA or Switzerland national identity card
- Firearms certificate or shotgun licence issued by a Police authority
- Northern Ireland voters card
- Council tax bill / demand letter*
- Notification of entitlement to state / local authority benefit *
- Notification of entitlement to tax credit *
- Notification of entitlement to pension from the DWP *
- Notification of entitlement to educational loan / grant *
- Notification of entitlement to other government / local authority grant *
- Instrument of a court appointment e.g. Probate or Court registered Power of Attorney
- HMRC (Inland Revenue) coding / assessment / statement / tax credit *
- Bank statement (not internet printed) **
- Credit card statement (not internet printed) **
- UCAS letter (student's only) *
- Local council rent card or tenancy agreement *
- HMRC (Inland Revenue) correspondence including name, address & permanent NI number *
- Pension / benefit correspondence from DWP *
- Utility bill (not mobile phone, satellite / cable TV or internet printed bills) **
- Confirmation from work / school / college / university / care institution confirming name, address and details of employment / student / residence status (students only) *
- Disclosure certificate issued by appropriate UK Agency, in the last 12 months. (UK Citizens only)

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

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

8.2 Appropriate persons

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

JMLSG guidance provides examples of applying measures, such as:

- Ensuring that client identity is established by additional documents, data or information
- Supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a financial services firm in the UK, EU or an equivalent jurisdiction

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

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

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

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

Seen the original of the endorsed copy document

and

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

The endorsing party should provide details of their occupation, employment contact address and UK contact telephone number (not being a mobile number). This information should be used by Compliance, on a risk-based sample or other selective basis, to validate the bona-fides of individuals who certify copy documents.

An individual whose personal endorsement (as above) on a client's copy documents, is acceptable when at the time of providing such endorsement, the person holds or carries out one of the following professions/offices in England, Wales, Scotland or Northern Ireland, or a recognised similar office in an EU state:

- Articled clerk of a limited company
- Assurance agent of recognised company
- Bank/building society official
- Chairman/director of a UK incorporated entity
- Chartered accountant
- Civil servant (permanent)

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

9. Anti-Bribery and Fraud Prevention

9.1 Anti Bribery

The Bribery Act 2010 provides legislation that consolidates and updates previous anti-corruption law with new criminal offences, covering bribery in both the public and private sectors. The act sets out the circumstances in which individuals may commit an offence of bribery. Generally, these are:

- Offering a bribe
- Promising to pay a bribe
- Giving a bribe
- Asking for a bribe
- Agreeing to receive a bribe
- Receiving a bribe

In addition to this, it is also an offence for a company to prevent a bribe from occurring.

There are six principles that every company should adhere to in relation to the Bribery Act:

- Principle 1, Proportionate procedures. The company's procedures to prevent bribery should be in proportion to the risk it faces
- Principle 2, Top-level commitment. All senior management should be committed to preventing bribery from occurring
- Principle 3, Risk Assessment. The company should perform regular risk assessments with the aim of determining the risk of bribery occurring
- Principle 4, Due diligence. All staff members should exercise extreme caution when performing their duties and adhere to company procedures
- Principle 5, Communication and Training. All staff should be aware of the regulation and be appropriately trained
- Principle 6, Monitoring and review. The commercial organisation monitors and reviews procedures designed to prevent bribery and makes improvements where necessary

The Company's Board takes the ultimate responsibility for ensuring that any risk has been contained by the firm. In order to reduce the risk, the company should implement Anti Bribery policies, gifts and hospitality policies, provide the necessary training and conduct risk assessments.

9.2 Fraud Prevention

All personnel are expected to draw to the attention of senior management any activity that is suspected of being fraudulent. This includes, but is not limited to:

- Falsification of records
- Forging of signatures
- Involvement with bribes (in accordance with our anti-bribery policy)
- Breaches of anti-money laundering procedures
- Any financial crime
- Misleading representations

Senior management will investigate and act in respect of any reports and will in addition notify the appropriate authorities.

9.3 Fraud Prevention Procedures

The actions taken in respect of any suspicion of fraud will depend upon the precise nature and circumstances. In all cases the first point of reference is your line manager.

Line managers must escalate the matter if it cannot be established that no fraud has occurred.

Senior management will investigate and consider the following in arriving at the actions to take:

- Notification to the FCA
- Report to the police
- SAR reporting to the National Crime Agency
- Disciplinary action in consultation with employment law support services

A full record of the investigation will be kept in a confidential environment as appropriate to the specifics of the case.

10. Training

10.1 Mandatory

Where an employee is found to have had reasonable grounds for knowing or suspecting money laundering, but failed to make a disclosure, he will have a defence under POCA if he does not know or suspect, and has not been provided with AML training by his employer - No such defence is available under the Terrorism Act.

Training is therefore mandatory and is an essential element of PAYPORT UK's financial crime arrangements. Training includes the following:

1. KYC and AML training within 15 days of beginning employment

2. Complete annual KYC and AML training
3. Reviewing and where necessary, updating training materials at least once per year
4. Training should include:
    a. Procedures to spot and deal specially (e.g. by referral to management) with situations that arise that suggest a heightened money laundering risk.
    b. Raising awareness of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through PAYPORT UK
    c. Raising awareness of relevant legislation, and employee obligations under that legislation
    d. How to operate a risk-based approach to anti-money laundering
    e. Arrangements for exception reporting by reference to objective triggers (e.g., transaction amount)
    f. Details of PAYPORT UK's responsibility
    g. How to recognise and deal with potential money laundering or terrorist financing transactions or activity
5. Training could include scenarios/case studies relevant to PAYPORT UK's business
6. On the job training for all on-boarding staff in the following manner – during actual onboarding activities, MLRO is taking staff through various onboarding processes for clients of differing risk and business profiles to assist in learning on how to apply policy and procedures in practice

10.2 Temporary personnel and Contractors

With regard to temporary personnel and contract staff ('casual personnel') employed on PAYPORT UK business: Unless subject to an exception approved by PAYPORT UK, when administering business relationships with, or facilitating unsupervised transactions for the benefit of account customers, one-off relationships or other third parties – casual personnel must attend relevant training and comply with PAYPORT UK AML requirements (per this Guidance).

10.3 Training records

Training records should be maintained, to document:

a. Details of training undertaken by each employee
b. Evidence of monitoring and review of employee attendance at training
c. The steps taken by management to ensure completeness of training attendance
d. The pass rates of employee training is to be kept to assess the effectiveness of training provided

Appendix 1

Use of electronic identification checks

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

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

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

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

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

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

PAYPORT UK

Appendix 2

Notification of Suspicious Activity

Form A

Client Name: _____

Client Account Number: _____

Client Address: _____

_____

_____

Grounds for Suspicion: _____

_____

_____

_____

_____

Date and Time of Activity: _____

_____

What Follow-Up is Required for the Client? _____

_____

_____

Employee Details:

Your Name: _____

Your Signature: _____

Date of report: _____

Nominated Officer signature[3]: _____

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