Good Practice Guidance for Member Firms

Topic: Anti Money Laundering programmes for FX firms

Date published: September 2019

Date for Review Q3 2020

About AFEP

Founded in 2012, AFEP work on behalf of their members to be the representative body for Authorised Payment and Electronic Money Institutions. Our mission is to elevate the standards of the FX and e-money industry, and advocate on behalf of our members with regulators & government bodies.

Background

In August 2018 the FCA opened consultation on applying the FCA's Principles for Businesses to payment services and e-money sectors, as well as applying communication rules to advertising and communication (CP18/21). The outcome of this consultation was issued on 1st February 2019 by the FCA as the 'General standards and communication rules for the payment services and e-money sectors' (PS19/3).

In preparation for this in late 2018, the AFEP Executive Committee began writing industry guidance on several key topics to act as good practice for our industry. As this good practice guidance has significant impact on how FX, e-money and payment services firms are encouraged to operate and how AFEP works with the FCA, AFEP worked with members to write this good guidance through working groups and Round Table sessions.

Good Practice Guidance documents have been written and issued to members on the following topics:

1. Communications with customers (currency convertors & disclosure)
2. Safeguarding
3. Customer interests & Conflicts of interest
4. AML
5. Corporate Governance

AFEP recognises the importance of members not only adhering to FCA and other legislation but also these Good Practice Guidance documents. Member firms are required, as a condition of membership, to confirm they are using the Good Practice Guidance and applying it to their business to ensure quality and compliance with the regulations.

This is high level guidance as it is for each firm to determine how to comply with the requirements as relevant to their business model. This guidance is intended for Authorised Payment Institutions (API's) and Authorised Electronic Money Institutions (AEMI's) who are full members of AFEP. This guidance is designed to assist members, and the FCA approach documentation and legislative requirements should always take priority. Members are encouraged to take their own independent advice to ensure they are meeting requirements.

Specific Legislative Background

This is topic specific legislative information about what regulations and requirements are already in place regarding Anti Money Laundering. It is primarily concerned with the obligations of the firm under the:

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
- The Proceeds of Crime Act 2002
- The Criminal Finances act 2017

It also considers the following guidance which is issued to industry:

- JMLSG Guidance, Issued by the British Bankers Association.
- Financial Crime: A guide for Firms, Parts 1 and 2 by the FCA
- Money Service Business Guidance for Money Laundering Supervision, by HMRC.
- Various guidance documents issued by ACAMS and other industry publications.

Objective

The objective of this good guidance is to raise standards in relation to key risks regarding Money Laundering:

Examples of Good Practice/Poor Practice

To assist member firms with applying this good practice guidance, several examples of good and poor practice are outlined throughout the document.

1. Board Approval

Core to any AML programme is that is receives the support and backing of the firms senior management. An AML programme which is being applied reluctantly or which is forced to make concessions is of limited use.

AFEP expects that all firms have a written set of documents, which meet the requirements and recommendations outlined below and which are seen and approved by the board. This approval, and the support of the board to enact and abide by these policies should be recorded in the board minutes.

2. Risk Assessments:

The basis of any firms AML control programme should be the conducting of risk assessments, which allow the firm to assess the levels of risk in its Customers, Countries and Geographic areas in which it operates, its products and services, its Transactions and its Delivery

channels[1]. Based on these risk assessments, the firm can identify key risks, weaknesses and gaps in its AML control programme.

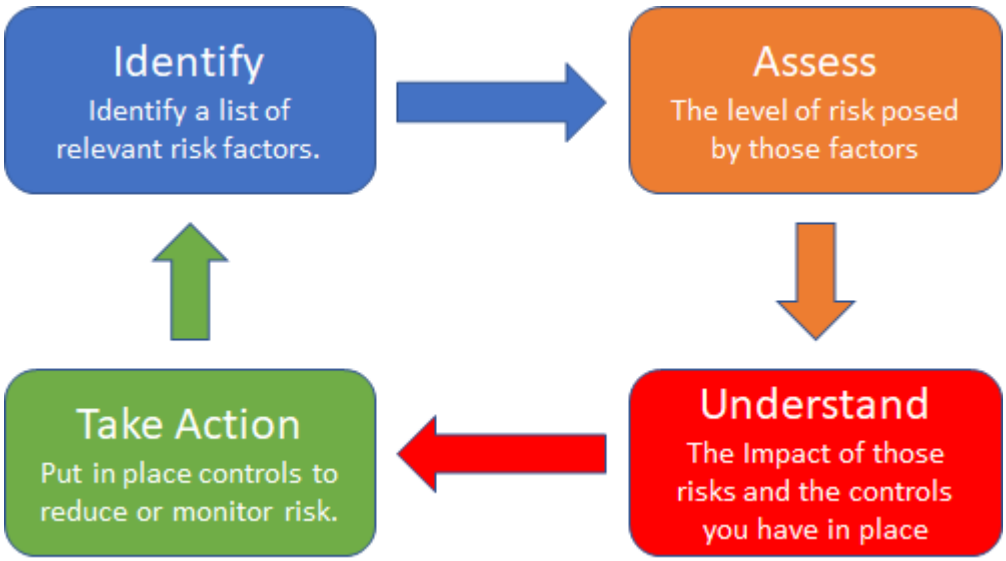
Based on these assessments the firm can then concentrate its resources on those areas in which the most benefit can be gained with the application of those resources.

Firms should ensure that these risk assessments are written and, once completed are kept up to date and accurate, reflecting the risks of the firm and are in keeping with the risk appetite of the firm. Firms should also ensure that the risks faced by the firm are appropriate to the level of resources and controls that the firm has available to it.

Ongoing process for risk assessments:

AFEP believes that the core foundation of a robust Risk based approach comes from an ongoing cycle of risk assessment as outlined in FATF recommendation 1:

"A robust risk process aims to identify, assess, and understand the money laundering and terrorist financing risks for a firm, allowing them to take action, based on that assessment, to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified"



This means that following the risk assessment, the firm needs to ensure that it monitors the outcome of the assessment and of the relevant reviews they are undertaking. This could

[1] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Section 18.

involve, as a minimum, reviewing the product risk assessments which have been considered for each product and assessing the controls which have been implemented. It may also mean that new products which are considered to be high risk but have board approval before they are offered to clients.

With the application of proper controls a product may become lower in risk. As extra features which are attractive to criminals are added, a product may become higher risk. A firm's board should be cognisant of those risks and before any change to a product is made, a risk assessment should be carried out to assess the impact of those changes to the firm's risk appetite.

3. Risk Appetite

Firms should also ensure that they have an established risk appetite, which is defined and approved by the board and establishes an allowed and accepted level of risk for AML across the board.

This should define limits on the risk level of products, define if the firm is seeking High or Low risk business, specify any areas of allowed business operations based on geographic risks and also should define the monitoring, control and responses to those risks.

For example, the risk appetite may define that the business is allowed no more than 10% of clients which are ranked as high risk, or may define that when a firm has more than 10% high risk clients, that it will increase its compliance budget to allow for additional monitoring and controls.

Feedback should be given to the board which provides details of how the firm is currently performing compared to its risk appetite, if it is operating inside of the parameters of the risk appetite and to make recommendations to remove or reduce risks as needed such that the firm continues to operate inside of its risk profile.

It should be noted that nothing prevents the firm from specifying that it has a high risk appetite, so long as it is able to put appropriate controls in place to mitigate these risks. Whilst firms should avoid considering cost and or profit margins as part of their risk assessment processes, it may be noted that firms can charge a premium for handling higher risk clients and sectors, particularly when they are able to demonstrate a higher level of controls over such sectors.

4. Product Risks:

In order to consider the attractiveness of a product to criminals, firms should look a products features, including ease of account opening, the flow of funds in, ability to hold or move funds internally inside of the firm, options for taking funds out and the level of monitoring present.

An ideal product risk assessment will consider the full lifecycle of a product, from ease of opening through to the features of the product when the client is using it in order to fully consider its risks.

By way of an example, if we consider two products:

Cash ISA	Current account
CDD Requires provision of National Insurance Number	Full CDD is carried out before account is opened.
Deposits accepted only from account in account holders name	Accepts third party funds in.
Does not accept cash deposits	Accepts cash deposits
Cannot withdraw cash	Can withdraw cash.
Funds cannot be remitted overseas	Funds Can be remitted overseas.
Limited volume and turnover on account	Unlimited turnover on account
Limited to one account per individual	Can have multiple accounts
Simple product type with limited functions, easy to monitor	May involve multiple bundled products, such as debit card, mobile banking etc, which need to be monitored.

We can see from this that a Cash ISA has less features or functions which are attractive to criminals. This is in part due to the very limited nature of the product offering, coupled with the levels of due diligence required at account opening and the levels of controls in place.

Based on this a cash ISA looks like a lower risk than the full service of a current account. However in order to properly assess a product, work should be carried out to assess each of the factors above and to decide if these are beneficial or attractive to a criminal.

To do this, firms should compile a list of risk factors, which they will then consider for all products (Even those that do not have that feature, these will simply score as low risk for that question) such that risk scores can be compared across their entire suite of products.

Factors to consider:

The following is a non exhaustive list of risk factors which might need to be considered as part of a product risk assessment:

- **Anonymity:** Both in terms of who our client is and who they are receiving funds in and from. There is a scale of anonymous, such that cash deposits into your bank account may be fully anonymous, card payments may yield some information and a wire transfer will give you details of the original remitter.

- **Cash:** Which can enter the firm from multiple angles depending on how the firm handles settlements. Is this something which is hard blocked in all accounts, preventing deposit or is there a risk of it entering via alternative methods.
- **Features of the product:** The more features that a product has, the more attractive it may be to criminals. But some features, for example, wire transfers, might be more attractive than others.
- **Monitoring;** What, if any, level of ongoing monitoring is there as part of the firm's ongoing product offering. A lack of monitoring or querying of the clients transactions is likely to represent a much higher AML risk than a product which has ongoing, live monitoring of transactions, or which prevents out of profile transactions from taking place.
- **CDD Process**; What level of CDD is required for the product, is there a requirement for EDD for the product (Low risk) or is there an SDD allowance? (Higher risk)
- **Funding Sources:** How can fund can be deposited with your institution will result in a range of different information from the sender. Firms should assess whether this information is verified, or if the user self submits names which cannot be checked (e.g. Card payments)
- **Thresholds and Limits:** Are there any restrictions or spending limits aplied, including lifetime limits and one off transaction limits which may encourage or detract criminals, or make the tool of limited value. How are these thresholds decided.
- **Ability to hold multiple accounts:** Is it possible to hold multiple accounts with your firm, in the same name. Does any process exist to detect multiples of the same type.
- **Destination of Payments:** Is it possible to send payments only to low risk countries, only to send domestic payments, or is there a capability to send payments to any country in the world. Do specific controls exist on each payment depending upon country risk?

A firm could then map the risks scores for all products against each other, targeting those products and risks which have a score of 5 and which are considered as posing a higher risk. The following is a fictitious sample table of risks and products:

Product	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5
Remittance	1	3	4	3	2
E-tailers	4	5	4	3	3
E-MoneyWallets	1	2	4	2	1

From this we can also see that Risk 1 is present only within E-tailers, Risk 2 is more prevalent for E-tailers, and risks 3 is present across all products.

The firm should thus look at why E-tailers have risks in some areas when other products do not, as this may indicate that the product has weaker controls. They should also review why risk 3 appears to be higher for all products, as this may indicate a general lack of controls for that risk.

It may also represent a specific product feature which the firm is aware of but wishes to retain.

5. Client Risks:

Client risk assessments seek to identify elements about a Clients which may imply a greater risk of money laundering, for example those individuals with political connections may be more prone to a risk of corruption, whilst firms which have been recently established and have no trading history may be more likely to be used for corporate abuses.

Risk assessment may also need to consider different risks between Individual and Corporate accounts, reflecting the different factors which can be considered.

Client risks should be considered prior to onboarding of the client, based on information which is available to them, but should also ensure that where additional information becomes available to them throughout the clients relationship with the firm, that this information is reflected in the firms client risk assessment.

Factors to consider as part of a client risk assessment:

The following is a non exhaustive list of risk factors which might need to be considered as part of a product risk assessment:

- **Individuals V Corporates:** Different risks will exist between corporates, for example corporates which have been established for a long period are more likely to be verified against public records, whereas individuals who are over a certain age may become more susceptible to being defrauded.
- **Industry Type:** Certain industries may be more susceptible to criminality, particularly if the industry has prior associations with criminal activity of if there are inherent risks associated with that industry. For example, firms involved in mining will often deal with land rights, which exposes them to a corruption risk.
- **Corporate entity type:** Some legal structures, such as Limited Partnerships have less transparent organisational structures or are able to hide their ownership or control, whereas some other entities are required to more prominently display their ownership and control structure.
- **Political Affiliations (PEP's, Government Contracts):** Access to politicians or working closely with governments as a supplier may increase the risks of bribery and corruption associated with such firms.
- **Age of the client:** Firms which have been established for a longer time are more likely to have publicly available information, have a more verifiable business activity and online presence and easier to validate via accounts. Ages for individuals may reflect vulnerability or concerns for the firm as to the source of the clients wealth if they are particularly young.
- **Geographies of the client:** The firm should link this to its geographic risk assessment and should consider the location of the firm, but also the expected destination of its payments and the ownership structure of the firm, as those firms which have ownership structures in higher risk countries may be attempting to utilise the lack of transparency for corporates in those locations.
- **Cash intensive businesses:** Whilst your firm may not handle cash, if your client is likely to receive large volumes of cash in, this may represent an increased risk that you firm will be remitting criminal funds overseas on their behalf.

- **Face to Face Clients:** Verification of clients on a face to face basis allows validation of their business activity and may help prevent impersonation fraud. Clients who have been met only on an Arm's Length or online basis may pose an increased risk.
- **High Net Worth Individuals:** High Net worth Individuals may pose an increase risk of tax evasion or corruption, it may also be harder to validate their source of wealth, the risks of which should be considered.
- **Who the Client Intends to Pay:** Payments back to the firms own account may pose a lower risk as it is easier to validate the recipients account. Payments to third parties may be harder to validate and pose a higher risk, particularly depending on where the client intends to pay.
- **Complexity of the ownership structure:** Complex or obscure ownership structures which may impede the ability to establish the UBO of a client may be indicative of a higher AML risk, whereas those firms with simple structures may pose a lower risk.
- **Ability to validate the clients business profile:** Is it possible to see a clear proof of activity, such as a well established website with reviews of the client, which links to the business activity which the client expects to do with you. Do other sites refer to you prospective clients business.
- **Negative news and press coverage:** Is there any publicly available information which would highlight concerns with the clients business or activities. Are these concerns major or minor, do they relate specifically to AML concerns.
- **Products and services to be used:** Firms should consider the products and services a client intends to use, and whether this is in keeping with the clients risk profile and the expected usage of the account

Ongoing Risk Assessment:

Client risk assessments should be updated to reflect the actual usage of the clients account as well as changes or updates which are made in the clients profile or their corporate fillings. For example if the client changes ownership, relocates to a new geography, diversifies into a different industry or changes the expected or actual usage of their account, does this impact their risk score.

Ongoing monitoring of client accounts should be established to ensure that such changes are noted and that they have an impact on the risk scores of your clients.

6. Geographic Risks

Geographic risk assessments seek to identify risks associated with differencing geographies, locations and jurisdictions which may impact a relationship with the client.

Such an assessment will need to consider a range of factors, such as the levels of regulatory control, levels of criminality and corruption in those geographies, as well as any international sanctions or controls over those locations. Other factors, such as favourable tax handling may also need to be considered.

In order to properly assess the geographic risks posed, firms may need to consider geography in multiple locations and not just the registered office location of a perspective client. Firms should consider:

Risk	Summary
Registered location of the client	This will be either the registered home address or the registered office address of the client.
Operating address or location of the client	Where the client trades from or primarily operates from an address which is not the same as their registered office address, it would be beneficial to note this discrepancy and consider if this address is in a different geography to your clients Registered address.
Location of key shareholders and management	Where the key shareholders are located in a different geography to the company, this may represent a different risk profile.
Destination of payments	Payments to higher risk jurisdictions, such as those with poor AML controls, may place criminal funds out of the reach of EU enforcement bodies. Higher risk locations may also increase the risk of corruption and other criminal activity, depending on the risks posed in the receiving country.
Source of Funds	Similarly to destination, firms should consider the specific risks of the countries from which they receive payments. .

Factors to consider as part of a Geographic risk assessment:

Several lists already exist which are commercially available and provide a documented methodology to assess geographic risk. Such resources take into account multiple sources and weight these against each other in order to establish a scorecard of countries.

Firms should ensure that they are not basing geographic risks solely on a single list or factor, such as corruption, but instead are taking into account a range of factors which are relevant. This may involve the development of an aggregate score card from multiple sources.

Firms should also be wary of the quality of sources which are used and should understand the methodologies and limitations of those lists, to avoid "Finger in the air" style risk assessments which are compiled from unrecognised sources.

The following is a non exhaustive list of risk factors which might need to be considered as part of a product risk assessment:

- **Corruption:** High levels of corruption in a country may indicate that it is easier to bribe officials and to hide funds once they arrive into a country. It may also reflect a lack of policing and controls in the country which make it easier to hide funds there.

- **Regulatory Controls:** A lack of regulatory controls in a country may simply mean that the movement of funds to that location is unlikely to be spotted, or that once they arrive it will be easier for a criminal to forward them on.
- **Current war or uprising:** Countries which have current disputes or socio-political issues are less likely to dedicate time and or resources to financial services controls, this may represent a weakness which can be exploited by criminals.
- **Narcotics:** If the country is known to be a supplier of narcotics, or a known transhipment point? this may increase the chances that a clients payments relate to narcotics or similar.
- **Terrorism:** Countries which are known supporters or sponsors of terrorism should be considered to pose an increased risk.
- **Tax havens or beneficial jurisdictions for tax handling:** Does the jurisdiction have a known favourable tax regime which would make it attractive to criminals or those seeking to move their resources offshore to avoid tax.
- **Sanctions or Restrictions:** Are there currently any sanctions or restrictions to doing business in the country.
- **Human Trafficking:** Is the country a known source for, or a transhipment point, for the movement of forced workers.

7. Delivery Channel Risk

Delivery Channel risks are those associated with how the client gains access to goods and services offered by your firm. In the past the primary focus of regulation has been around concerns over Non Face to Face relationships and the increased risk of impersonation fraud.

Firms should now be considering whether their use of Agents or other intermediaries and correspondents reduces the oversight that they have of a customer or transaction, or if the additional steps and intermediaries limit the application of controls which they would usually be put in place when a client was dealing directly with the firm.

The following is a non exhaustive list of risk factors which might need to be considered as part of a delivery channel risk assessment:

- **Face to Face Relationship:** Was the business conducted on a face to face basis, with a meeting with the client. Have you visited or seen their place of work, or was the meeting conducted in a hotel/coffee shop rather than at the place of business. Did any form of verification of the clients business take place by your sales staff?
- **Use of Agents:** Did the client journey include any sort of agent or intermediary who performed a part of the compliance or payments process on behalf of your firm? What autonomy or risks exist through the use of that intermediary.
- **Source of the Client:** Was the client sourced form an introducer, white label or some other introductory method which you place reliance upon to perform some part of the due diligence. Does your risk scoring process consider the use of intermediary's and brokers a higher, or a lower risk?

- **Reliance:** Was the client introduced by another firm in your group, or another regulated firm which conducted due diligence on the client upon which you place reliance.
- **Third Parties and Correspondents:** Are you providing a service to the end user, or to a correspondent bank or other FI. What level of regulation is placed upon that FI, and how often is this audited and or reviewed. What jurisdiction is that FI in and what level of reliance can be placed upon their licence.
- **Access to Data:** Based upon the relationship flow that you have and any restrictions which may exist, how easy or hard is it for your firm to obtain data on the underlying client if needed. Is data stored directly into your systems, or would this need to be requested. Will this impact your ability to conduct CDD, EDD or monitoring?

Firms should conduct a delivery channel risk assessment upon all of the channels which they currently have in place, and where a new channel/agent/intermediary is introduced, should seek to assess the relationship with this new partner and assess if this channel is identical to prior processes. This will prevent instances where a new partner is introduced with weakened controls or which blocks oversight of a key AML element, such as source of funds checks.

A delivery Channel risk assessment should thus be available for each Delivery Channel which is available. This may resemble the Product risk Approach, in which various channels are compared against each other based upon the risks identified, and the levels of controls which are available.

8. Mitigating Risks:

It should be noted that the aim of a risk assessment is not to drive risk to absolute zero as this is not possible. Any business which has clients will have some level of risk involved.

What is important is that the risk be commensurate and in keeping with the agreed risk profile as defined by the board. If a single product risk which is identified is considered to be the key feature of a product, then it may be decided by the board to retain that risk.

Where it is decided that it is beneficial to reduce the risk, the assessment should be used to drive some form of behaviour which reduces the risk score. The methodology proposed above, which is based on a 1-5 score, also acts to show us the controls which could be used. If for example a risk of 5 is identified, then introducing post event monitoring would move that risk to a 4, introducing pre-event monitoring would move it to a 3 etc.

The following methods could also be used to mitigate risks:.

- Prevent high risk clients from using high risk products.
- Requires that higher risk products have a stricter transaction monitoring ruleset.
- Requires EDD for any clients seeking to use higher risk products.
- Places limits and thresholds on high risk products
- Requires an annual review or board sign off for the product.

9. Customer Due Diligence

Customer Due Diligence (CDD) is the process bn which a firm must Identify the customer, and to verify, on a risk sensitive basis, the identity of that customer, such that they have sufficient documentation on the identity of that customer. The firm must also understand the intended nature of the business relationship.

This means that firms should be able to clearly prove that they know who the client is and what they will be using the services of the member firm for. Such information is required from the outset and on an ongoing basis throughout the business relationship.

In this context a business relationship is a business, professional or commercial relationship between a member firm and a customer, which the business expects, on establishing the contact, to have an element of duration. It is the opinion of AFEP that where you set up a customer account, give a unique customer reference number, or permit them to perform transactions with your firm, that a business relationship has been established.

A relationship ceases at the point at which the account is closed (either by the firm, or at the clients request) and at the point where it is no longer possible for a client to utilise the services of the member firm.

In light of the creation of a business relationship AFEP does not believe that member firms are able to rely on the EUR 1000 limit in the wire transfer regulations and therefore must perform CDD on all customers. The level and nature of this Due Diligence may be affected by Simplified due diligence (SDD) allowances, but SDD should not be confused with a permission to perform no CDD.

The CDD process must be completed prior to the receipt of funds from a customer. In practical terms this means an FX broker could allow a potential client to book a deal but must have completed CDD prior to accepting funds in or making onward payment. Obviously there is an exposure risk on the booked deal should the client be rejected as a result of them failing the CDD Process.

Due Diligence Requirements

Customer Due Diligence requirements should be distinct and recognise the different forms, structures and types of a client which a member firm may trade with.

It is not sufficient to conduct CDD only on an individual director who represents a firm in order to trade with a corporate entity. Similarly the details of a business or corporate entity may not be relevant when a firm is clearly trading with an individual. Firms should establish a clear CDD policy which defines the documents, identification and supporting information which is required for each legal entity type which they are looking to trade with.

It should be remembered at all times that the intention of Due Diligence is multi-faceted. It seeks to ensure that where a client turns out to be a criminal, that sufficient information is held on that individual such that investigating bodies are able to locate them; but also to ensure that firms hold sufficient information on their clients that they are able to spot red flags or suspicious activity where it arises.

Firms which concentrate too heavily on who the client is, but do no checking of what the client does or why they have a relationship with a member firm, risk being unable to properly monitor a clients account and detect criminal behaviours. Firms which operate a tick box approach to checks are also likely to miss nuances and indicators specific to the clients business or transactions which could be indicative of criminality.

1. Individuals

CDD for an individual should be based on reliable source, independent of the customer, which is based on documents, electronic checks or a combination of both, such that the firm has verified the following information in relation to their clients:

- Full Name
- Residential Address (not a service or correspondence address)
- Date of Birth

Firms should also ensure that that they are dealing with the individual who is presenting the documents (Anti Impersonation checks) such that they are confident that they are not creating fraudulent accounts or trading with a front or agent representing an underlying client. This means that reliance solely on the client providing the above data which is then verified by Electronic Verification may not be suitable.

AFEP's standard requirement for documentary evidence for non face to face clients is to obtain a minimum of one document to verify the ID (Name, DOB) of an individual and one document to verify the address, plus one additional ID or address verification.

For Face to Face client verification, a single Identity Document may be obtained, along with a single Address verification document from those listed below.

Documentary Evidence:

For the verification of Identity (Name and DOB) firms should obtain a Government Issued ID, including a photograph of the individual. These can include:

- Passport
- Photocard Drivers Licence
- National ID Card
- Firearms Certificate
- Shotgun Licence
- ID Cards issued by Electoral Bodies.

For the verification of address, the following documents may be provided:

- A recent (Less than 3 months old) statement issued by a bank or institution regulated by a competent EU authority.
- A recent (Less than 3 months old) Utility bill, issued by a power, energy or utilities provider
- A council tax bill for the current year

- A TV Licence
- Photocard Drivers Licence, where this has not been used to verify the clients address.
- Physical attendance at the address of the customer by a staff member, if certified by staff

PDF and Online Statements are acceptable and reflects that a growing number of individuals no longer receive paper statements of their accounts. Firms should take into account the ability for electronic documents, or for photos and copies of documents, to have been tampered with and ensure that relevant checks are in place to verify any documents which are accepted in PDF form.

Any documents provided should be –

- Valid and in Date
- Should include the individuals name and DOB
- Be clear copies which have not been redacted in any way
- Copies should show all 4 corners of the document to aid in verification
- For Drivers Licences, show the current valid address of the client
- All data on the document should match against other data provided
- Where in a foreign Language, translated and verified accordingly.

Copies of documentation used to verify a clients identity should be stored, not just reference numbers or other proofs of verification.

Where a client is considered to be higher risk, or where the situation may necessitate it electronic verification can be used.

Electronic Verification

Electronic verification utilises databases of information from credit referencing agencies and other sources to confirm that a person with the name given has a credit footprint at the address provided.

Prior to placing any form of reliance upon an Electronic Verification identity provider, firms must ensure that they are comfortable with the level of checks which are carried out by the EV provider, to ensure that they are fully aware of the level and depth of any checks carried out, the sources of such checks and the passing scores which are used in order to accept a client. Firms should ensure that the EV provider, and any reports or outputs which are used to verify clients:

- Utilises multiple data sources to obtain information which is then corroborated against each other.
- Utilises data sources which are independent of the client (As opposed to utilising social media which was user generated)
- Has the ability to monitor data across time, such that if a clients address is no longer accurate, they are able to detect that an individual may have since moved on.
- Can incorporate qualitative checks (not just quantitative) to assess the strength of information provided and to detect discrepancies
- Can provide scoring or display to the end user how a decision was made, or what sources were used to make a decision on a client.

- Can reflect negative sources, such as CIFAS or the Halo Deceased register which may detect fraud or other negative flags on the client. Systems which can also detect a high volume of applications in a single clients name by multiple flags are also advantageous.
- Is registered with the ICO as a credit referencing agency or utilises data from those bodies in order to ensure that it maintains a minimum standard of data/controls.
- Has controls in place to prevent underlying users from amending the passing scores of customers.
- Are sufficiently granular that the firm is able to tell which elements of a clients data (Name, Address, DOB) have been verified, rather than presenting a purely Pass/Fail result.

When setting up the "Scorecard" which defines if a client has passed Electronic Verification, AFEP believes that an individual should be matched against: a minimum of 3 matches to a client's name through electronic verification i.e.:

- Name + Two addresses and one date of birth
- Name + One address and two dates of birth

Firms should ensure that they are able to detect which elements have passed, in order to rule out incidents of name matching.

A copy of any data used in the verification of a client, including the output and any subsequent reports should be saved for record keeping purposes.

Real Time Electronic verification:
Real time ID verification is a Hybrid approach between Documentary Evidence, Electronic Verification and Face to Face verification.

In this scenario a firm may capture documentary evidence of a client, as well as a short video or selfie of the end user, confirming that they do indeed match the photo on the ID provided.

Such systems are often automated, utilising facial recognition software to match individuals, as well as other tools to ensure that users are not simply presenting a high quality photo of a fraud victim, in order to trick the software. Such firms will also often have a "Fall back" process, which allow a human to intervene when such systems fail.

Prior to utilising any such vendor, firms should consider the technological merits and processes of such a system, to understand how these systems operate, the relevant passing and failing metrics utilised and the processes which they operate under. As a minimum, firms should consider:

- Whether the system has in place adequate controls to prevent users from faking documentation or obscuring falsified information
- The controls which the system has to detect whether the individual is indeed the same individual as pictured on the ID.
- Whether any external, negative source materials are utilised in the verification, or if reliance may be placed on a single document
- The level of checks carried out on various document types, including any checks against external databased of falsified documents

- What information is verified during the processes. For example how such systems, when utilising a passport, may or may not verify the address of the user.
- The amount of data which is presented to the firm to prove that validation took place.
- The ability to recall data, such as videos or photos of users which are taken, if the firm ceases to use the vendor.
- Whether the level of checking carried out is sufficient for the firm, based on the risk and nature of the products that the client will be using.
- What other checks are possible in the tool, such as conducting source of wealth checks or confirming the nature and purpose of the clients account, or if these are not available, how will the firm conduct these?
- What is the process if a user fails to pass automated checks, who is responsible for conducting additional checks, or will a human intervention process take place by the firm.

It is noted that an off the shelf product may be suitable for the firm to use, however this should be considered inside of the scope, nature and risk of the firm to ensure that the tool is appropriate.

2. Corporates

A corporate client is any client who is a business or legal structure, representing something other than their own personal interests. They are distinctly different from individuals in terms of AML risk as the number of people involved in the corporate entity who may influence it or utilise it for criminal acts may increase when compared to an individuals account.

Corporate structures may also be used to conceal ownership or control of an entity and its funds, such that the person who purports to represent the firm at a business meeting may not have any final say in the business. Corporate structures may also be made unduly complex, or involve overseas jurisdictions, such that it is possible to completely conceal the ownership or control of an entity.

Member firms should ensure that their onboarding process is robust enough and has a process for each legal entity type which it encounters, such that when following its CDD process, it is able identify the legal entity itself, and to name those individuals who own and controls the legal entity.

In order to identify the legal entity itself, the firm should take steps to identify[2]:

- The full legal name of the entity
- Any trading or brand names which is may be using
- The registered Number, as held with the relevant companies registry
- The registered address in the country of incorporation
- The Principle office address, where this is different from the registered address.
- Any other registration numbers, such as VAT registration or Tax ID's where relevant in the country of incorporation.

Firms should take steps to verify the information presented to them by the client, for example by:

[2] Firms should consider guidance in S 5.3.152 of the JMLSG Part 1.

- Searching corporate registries which present publicly filled information.
- Utilising online resources to verify addresses, registration numbers and the location of the clients business.
- Verifying TAX ID's or VAT numbers using publicly available sources.
- Obtaining certified documents pertaining to the company, such as certified incorporation documents.
- Through the use of official documentation, such as VAT returns or tax bills issued to the client.
- Validating addresses through publicly available licence registries.

Firms must ensure that the information that they use contains information which is independent of the client, and thus reliance solely on a single point of information (such as the company registry) is not sufficient in order to meet a firms CDD requirements. Verification of such information should be sought from 3rd party sources.

Own or Controls means any individual who[3]:

- Owns 25% or greater than the shares or voting rights in the client entity.
- Exercises control over the business through their position in senior management,
- Or, Exercises control over via other means such as via a trust arrangement or representatives.

Firms should consider whether an individual with a shareholding of less than 25%, but who wields control via a trust, a senior management position or as a Person of Significant Control may also be considered as a controller of the entity, despite not clearly meeting any of the above elements explicitly.

Firms should also consider whether the structure, management or control of the business may be unclear or handled by another person based on the nature and form of the legal entity. For example where a trust arrangement exists, or whereby another multiple corporate entities control small segments of the business, it may be prudent to review the companies articles and to understand how the control of the business operates rather than making assumptions about the voting structure of the client.

Differences in the types, forms and structures of shares may be used to conceal ownership and should be taken into account. Firms should query whether the clients use of an overly complex or confusing legal structure is beneficial to the firm, or if this is being used for nefarious purposes. The location and style of corporate owners, for example where a client is owned by several other legal entities in higher risk jurisdictions should also be considered.

Firms are also required to understand the law to which the corporate entity is subjected to. This may be particularly relevant where the corporate entity in question is located outside of the UK or in a jurisdiction in which the member firm is unfamiliar with corporate requirements, or where the corporate form of the client is a lesser known legal structure which may be favoured by criminals.

[3] Firms should consider guidance in S 5.3.151 of the JMLSG Part 1.

Where firms are unable to establish an individual who owns a controlling share of the business, they may instead take steps to conduct CDD on the individuals who are responsible for the management of the business.

Firms should also be aware of the limitations of corporate registries, and should not that relying solely upon Companies house or another corporate registrar alone is not sufficient to meet the KYC standards as defined in the Money Laundering Regulations.[4] Corroborative evidence of some form including evidence of the businesses operations, history and proof of its control via internal documents and publicly accessible documentation should be obtained.

In addition to the above elements, the individual purporting to act on behalf of the client (The individual who is acting signatory of the application, form for example) should be verified in keeping with the requirements of identifying an individual, as defined above. Verification in this fashion seeks to prevent fraud and individuals from representing themselves as another business. Firms should also ensure that the individual in question has the authority to enter into arrangements and conclude contracts on behalf of the prospective client.

3. Nature and Purpose

In addition to understanding the individuals that a firm is dealing with, or the legal entity details, it is important that a member firm understands the Nature and Purpose of their new client and of the intended business relationship. This information will be used by the firm to ensure that the transactions which take place through the clients' accounts are in keeping with the profile, and that these transactions make commercial sense for the clients transactions.

This means that firms need to establish not only who the client is, but what they do as a and what they intend to use the member firm to do. As a minimum, firms should understand:

Individual Clients:

- The expected turnover and volumes which the individual will be sending
- The source of funds the client will be using, particularly where the transactions are larger, one off transactions.
- The expected destinations of payments
- The expected beneficiaries of payments, such as whether these are suppliers, lawyers, or other individuals that are being paid
- What the expected payments are for, e.g. if these are for investment, a house purchase, payments to family etc.

Corporate Clients:

- The business activity of the client, including the type of products or services which they offer to their clients.
- The industry that a client operates n and whether this industry is a known high risk industry.

[4] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, S28(9)

- The business model and distribution channels which the clients uses.
- Where in the value chain the client is, are they a wholesaler, retailer etc.
- The type and nature of the client's, for example are they primarily servicing vulnerable individuals or using certain sales techniques to attract clients.
- Any licencing requirements which may impact the firms business.
- The locations, geographies or regions in which they operate.
- Whether the business is cash intensive or whether it has any other indicators or markers of a high risk business.
- The expected turnover of the business
- The size and scale of expected transactions that the client will conduct
- The frequency of payments to be expected.
- The source of funds and source of wealth that a client will be utilising.
- The expected destinations of payments.
- The age of the client and the ability to verify the above information based upon publicly accessible information.

Once firms have obtained this information, they should attempt to verify this by open source research. For example:

- By confirming that the expected turnovers and volumes are in keeping with the accounts or bank statements provided by the client.
- That the suppliers or beneficiary countries provided are in keeping with the clients activity, for example it is unlikely that they are importing exotic fruits from Iceland or cars from Malta.
- That the information provided by the client is consistent in and of itself, for example the expected size of payments, volume of payments and annual turnover are all correct and add up to a reasonable amount.
- That the clients business activity can be verified publicly, for example a web shop or similar can be found, and this site appears to be active.
- That there are reviews or other forms of feedback available on the client, such that a credible business appears to operate in that fashion.
- That suppliers can be identified and reviewed in a similar fashion to the client, for example supposed law firms can be validated.

As an industry, and in line with JMLSG guidance, we believe that it is not always practical or necessary to obtain certified documents where original documents are not seen, provided that compensating controls or additional due diligence is in place for example one or more of:

- Funds received from a bank account or card in the name of the account holder
- Additional verification requirements of non face to face transactions (i.e. 3 separate ID/address documents or checks),
- Electronic authentication of copy documents

4. Ongoing Due Diligence

Firms should recognise that customer due diligence is timely, meaning that when it is conducted it reflects the firms understanding of the client at the time that CDD was carried out. The accuracy of CDD will decay over time, reducing its effectiveness.

Firms may need to periodically review and re-assess the KYC they hold on firms and individuals, to ensure that it is still accurate and reflects their understanding of the customer, the CDD they hold on their customer and the customers' needs and expected usage of the account.

Firms can take multiple routes to conducting ongoing CDD and a chosen solution should reflect the types of client a firm has, the risk of those clients and the level of information available about those entities which they can obtain on an automated basis:

Firms should also take this opportunity to ensure that CDD information held is in keeping with current legislative standards. Where regulations or laws have change or been amended since the client was onboarded, firms should ensure that they are holding a level of CDD which is commensurate with current legislative requirements.

Client risk rankings should also be kept up to date, and where the firm becomes aware that they risk profile of a client may have changed since it was originally calculated, steps should be taken to update this assessment whilst CDD is being updated.

When completing a KYC refresh, it is important that where possible old data is not overlaid or redacted, so that the firm is able to show the CDD which was originally conducted.

Ongoing Screening:

For corporate customers, firms may wish to setup an alerts process with the relevant company registry, or with a third party provider, which informs them of changes to the client's corporate information, for example changes to registered address, changes in Directors or in the persons of significant control.

Firms can use these changes as an alert in order to review the clients CDD.

Firms should be aware that the level of monitoring available for corporate clients will depend heavily upon the openness and availability of the corporate registry in the country of the client. Firms must not rely on this method when information is not publicly accessible.

It should also be considered that where a firm is located in a jurisdiction with an open registry, but its ownership or control rests in a location without such oversight, or where the ownership structure (such as through the use of a trust) does not afford such transparency, this method alone may not be sufficient.

This review should also be combined with ongoing transaction monitoring, such that the firm is able to confirm the Nature and Purpose of the account and that the client is using the service as intended or expected.

Risk Based Periodic Review:

Where firms are unable to automate the monitoring of clients, for example where they are an individual and there is no automated update as to their current address, or where the client is a corporate located in a jurisdiction which does not provide an automated update service, firms must have in place a process for periodically reviewing the KYC and information they hold on a manual basis.

This should be risk based, such that clients which pose a higher risk are subject to enhanced scrutiny and a more frequent level of periodic review. Firms should also consider if a product risk will increase the frequency of reviews, such that higher risk clients using higher risk products are subject to enhanced assessments.011

Such a KYC Refresh should involve a review of all information obtained during the CDD process, including, where appropriate, correspondence with the customer to confirm that all information held is up to date, accurate and is held in the appropriate location within the firm.

Events driven screening:
Where a member firm becomes aware that the information that they hold may no longer be accurate, it may be beneficial to trigger a CDD refresh. This may occur when:

- The client firm has a new contact who purports to act on behalf of the firm
- The client becomes known in the news or negative media screening, for example press coverage of a buyout or change in ownership.
- The client requests a change to the information held, such as an address update or similar.
- Transaction monitoring or alerting detects a change in the clients behaviours or trading pattern.
- Dealers or trading staff notice a change in behaviour or dealing process.

10. Sanctions Screening

Firms are required to ensure that they do not trade with, or make financial resources available, to those individuals or entities (Collectively, Specially Designated Nationals) who appear on certain Sanctions lists.

The specific sanctions lists which are relevant to member firms will depend upon the geographies and currencies in which they operate, and member firms are advised to ensure that they review the relevant lists on a regular basis to confirm that they are correctly screening against the right ones. Firms are also reminded that their banking counterparties may require that they screen against specific lists, on the basis of their locations and the regulations which define how they process payments.

As a minimum, AFEP would expect firms to be screening against:

- HM Treasury Sanctions Lists
- US OFAC list

- UN List
- EU Sanctions List.

During the course of the onboarding process, firms should consider how much information it is pertinent to screen. Sanctions legislation does not define a specific % under which screening does not need to take place, so firms should be aware that operating accounts for firms with a 20% shareholding by a sanctioned individuals is still likely to be a breach of sanctions law.

At onboarding, AFEP would expect firms to screen, as a minimum:

- The clients name, either corporate legal entity name or the name of the individual account holder. Where this is a joint account, the names of both account holders.
- The names of the directors and company secretary of any legal entity
- The names of any shareholders, including legal entities or parents.
- The names of any Controllers, where they are not directors or Shareholders
- The names of any authorised traders.

Subsequently, when the client trades, we would expect firms to screen:

- The details of any Beneficiary
- The bank of the beneficiary
- Any correspondent or intermediary banks to be used.
- Any onward forwarding or relaying instructions included with the message.

Timing of Screening

Sanctions legislation does not allow for a Simplified Due Diligence threshold. On this basis, Sanctions screening should take place before any transactions or trades are booked or executed for the client.

When making a payment, firms should have a hard stop, which prevents payments from being sent until they have been screened. There is little or no benefit in a firm identifying that a payment WAS made to a sanctioned individual if they have already released funds.

Similarly, firms should consider the freshness of screening. Screening which takes place when a trade is booked may result in the screening having taken place several days before a payment is sent. Updates to the sanctions list may have occurred in this time, resulting in the screening being out of date. Firms should be aware of when a screen has taken place and ensure that an up to date screening is conducted prior to the payment being released.

Ongoing and One off Screening

Vendors may offer a service in which they allow firms to conduct ongoing screening of a client, which allows them to notify the firm if a client or the individuals associated with a client become sanctioned, after the initial screening takes place.

Firms should consider whether they are required to screen certain names on an ongoing basis, or whether their screening should take place on a per transaction basis. It may be inefficient for

example, to conduct ongoing screening of beneficiaries who are due to only be paid once, as an alert in the future may be of limited benefit if the client no longer intends to pay that beneficiary.

Conversely ongoing monitoring of shareholders or directors at a client, and the name of the client itself, are likely to be beneficial if screened on an ongoing basis.

Firms should have a policy in place which clearly explores the decisions made, and the rationale behind choosing such processes.

Use of Fuzzy Logic

Fuzzy logic is the use of computer algorithms to detect words or phrases which are like, but not an exact match to another word or phrase. For example, if I sanctions screen the name Mike using exact matching, and Michael is a sanctioned individual, the system will not find a match.

If I utilise Fuzzy matching, the system may recognise that Mike is a common abbreviation of Michael and result in a match.

Fuzzy matching can be achieved in several ways, and firms should understand how the fuzzy matching of their chosen vendor works. They should test their systems frequently to ensure that they understand the parameters used and the matching rates which they are likely to see.

When firms consider a new jurisdiction, for example where they move from European style names, to certain Asian cultures which favour monosyllabic names, changes may need to be made in the matching rates in order to ensure the system is not generating an unworkable number of false positives, but also that it is correctly identifying sanctioned individuals Firms may need to consider multiple systems or changes to the systems they currently use.

Negative News and reputation screening

Many firms who operate Sanctions Screening systems also offer firms the ability to screen against Negative News or Reputation screening lists.

Unlike Sanctions lists, which are generated from official government lists, there is no official source for Negative News lists. Individual vendors will have their own methodology and criteria for inclusion of a news article, and may screen a variety of different news sources in a variety of languages. Firms should understand, as far as is possible, how their vendor compiles the lists that they are using.

Firms are encouraged to use negative news and reputation screening[5] in order to fully understand their client, but firms must understand the limitations of such screening. Vendors will only be able to provide information which is available from news and media outlets, once a conviction or report has been generated, they are not able to speculate or report on the reputation of firms without some evidential basis and may not comment on ongoing cases. This is because a vendor adding such names to a database may result in legal action by an entity if this were to unfairly prevent them from doing business.

[5] Annex 4-II JMLSG Guidance December 2017, Reputation.

Firms should consider the scope of the source materials that vendors are using and the alternatives and corroborative searches they could do, such as open media source searching or the use of forums and other materials to assess the reputation of an entity. Firms may also wish to consider the level of fuzziness that is applied to negative media searches, when compared to Sanctions searches.

For example, negative media screening is unlikely to take into account a large number of complaints on a forum about a beneficiary who is believed to be scamming elderly "investors", or a forum for soldiers of fortune asking if they should work for an entity which you are about to pay which offers guns for hire.

AFEP Members are encouraged to use multiple sources when considering the reputation of their clients, controllers, shareholders and beneficiaries. The firms policies and procedures should provide clear guidance and a process for analysts to use in order to conduct such searches, including details of how to record and resolve such searches where these are not found via the usual process.

Garbage In, Garbage Out.

The more data a system has access to, the better its matching capabilities. It is also easier for a system to differentiate based on a number (such as passport number, date of birth etc) than based on a name. This is because numbers tend to require less fuzzy logic and have less variations in them.

Firms should consider, where possible, how much data they are able to pass to a sanctions screening tool, in order to increase its efficiency and matching rates. Where they hold data, such as a passport or ID document for a signatory, this may be sufficient to clear a sanctions alert, if the system knows about this.

Firms should consider what data they hold, and submit this alongside the name of the individual being screened, if this is beneficial to their screening process.

Testing of systems

Firms should regularly test their sanctions screening systems, to ensure that the tools are stopping payments and flagging accounts as intended. Firms should consider using mock data or accounts to test not just that the system recognises relevant information when presented, but also that it is able to block accounts, halt payments and alert the relevant staff as intended.

Testing of fuzzy matching, including the use of deliberately edited names and pseudonyms, taken from the sanctions list and then modified is also considered to be industry best practice.

11. Politically Exposed Persons

Firms are required to have in place proportionate policies and procedures, such that they are able to identify Politically exposed persons (PEP's) who are, either direct clients (such as private Individuals or embassies) or where there is a PEP who is the owner or controller of a client.

It should be noted that when a PEP is a beneficial owner of a customer, it does not require that a legal entity should be treated as a PEP just because a PEP might be a beneficial owner. Firms should consider the potion held by the individual and their involvement in the firm for any high risk

indicators, for example a PEP who has the ability to assign mineral rights who also owns a mining company is likely to pose a high risk even if they are only a shareholder with no involvement in the day to day running of the client.

Firms should also be able to identify those individuals, who by virtue of their family connections and relationships, may have access to those PEP's and be able to influence them unduly, such as the Siblings, Parents, Spouse or Children of any PEP.

Firms should take a proportionate and risk based approach to PEP's, ensuring that the controls which they put in place to identify, conduct any relevant EDD and any ongoing monitoring of PEP's is proportionate to the position they hold, the functions which they perform at the firm and the risk assessments carried out by the firm[6] such as the firms own product risk assessments.

Firms should have a documented and specific PEP policy, which deals with the following considerations.

Positions Which qualify as a PEP:

Firms should note that the definition of a PEP is any individual which holds a **prominent** public function[7]. AFEP would expect firms to understand the nature of the position held and whether the function gives rises to the risk of large-scale abuse of position.

Firms should consider the risks posed in the country where the position is held and any additional risks which are posed by the PEP being located in that country. As a general rule, firms should consider the following positions as PEPs:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or of similar legislative bodies – similar legislative bodies include regional governments in federalised systems and devolved administrations, including the Scottish Executive and Welsh Assembly. It does not include local government in the UK but it may, where higher risks are assessed, be appropriate to do so in other countries.
- Members of the governing bodies of political parties – the FCA considers that this only applies to political parties who have some representation in a national or supranational Parliament or similar legislative body as defined above.
- Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances – in the UK this means only judges of the Supreme Court; firms should not treat any other member of the judiciary as a PEP and only apply EDD measures where they have assessed additional risks.
- Members of courts of auditors or of the boards of central banks
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces
- Members of the administrative, management or supervisory bodies of State owned enterprises, where the state has ownership of greater than 50%

[6] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 S.35 (2)
[7] FCA Guidance FG17-06 Page 6.

- directors, deputy directors and members of the board or equivalent function of an international organisation – The FCA considers that international organisations only includes international public organisations such as the UN and NATO. The Government made clear in their consultation of 15 March 2017 that they do not intend this definition to extend to international sporting federations.

The regulations exclude from the definition of a PEP those who are 'junior or midranking', however firms may wish to treat such individuals as PEP's where they work for, or are associated with a high ranking PEP, or where they are in a country in which large scale corruption would suggest that additional measures be taken, such as those with known high levels of corruption.

When a PEP ceases to be a PEP:
If a person who is a PEP is no longer entrusted with a prominent public function, that person should continue to be subject to risk-based enhanced due diligence for a period of at least 12 months after the date they ceased to be entrusted with that public function

High Risk PEP's:

Firms should consider, as a minimum, the following factors as being a higher risk, when assessing the risks posed of a PEP:

- Where the personal wealth or lifestyle of the PEP inconsistent with known legitimate sources of income or wealth;
- Where the PEP has failed to declare the interest or holding, for example they have not recorded their shares on the register of Interests in the UK.
- if the PEP is located in a country has laws that do not generally permit the holding of a foreign bank account, a bank should satisfy itself that the customer has authority to do so before opening an account
- Where there have been credible allegations made against the PEP of financial misconduct (eg facilitated, made, or accepted bribes)
- Where the PEP is responsibility for, or able to influence, large public procurement exercises, particularly where procurement is not subject to competitive tender, or otherwise lacks transparency
- Where the PEP is able to is responsible for, or able to influence, allocation of scarce government licenses such as mineral extraction concessions or permission for significant construction projects.

Lower risk PEPS:

Firms should also consider that some political positions will result in the individual holding limited power, or being unable to significantly influence decision making. Firms may consider that where an individual holds a position, but they or their position:

- Are subject to rigorous disclosures requirements (such as registers of interests, independent oversight of expenses)

- Does not have executive decision-making responsibilities (eg an opposition MP or an MP of the party in government but with no ministerial office)

A PEP may pose a lower risk and may be subject to less stringent controls.

Geographic considerations for PEP's:

When considering the risk of a PEP, firms should take into account the location of the PEP and of the position held. The following factors may be indicative of a higher risk political position, where they are in a country associated with:

- High levels of corruption
- Political instability
- Weak state institutions
- Weak anti-money laundering defences
- Armed conflict
- Non-democratic forms of government
- Widespread organised criminality
- A political economy dominated by a small number of people/entities with close links to the state
- Lacking a free press and where legal or other measures constrain journalistic investigation
- A criminal justice system vulnerable to political interference
- Lacking expertise and skills related to book-keeping, accountancy and audit, particularly in the public sector
- Law and culture antagonistic to the interests of whistleblowers
- Weaknesses in the transparency of registries of ownership for companies, land and equities
- Human rights abuses

EDD for PEP's

The level of EDD or controls which should be applied to a PEP should be based upon the level of risk which a PEP poses. Overly burdensome controls applied to mid-level council workers is not beneficial. Similarly, controls which are generic, and which are not specific to the risks of being a PEP, risk being ineffective and cumbersome.

Once a position as a low risk PEP has been established, firms should consider the following steps:

- Take less intrusive and less exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP;
- Oversight and approval of the relationship which takes place at a level less senior than board of director level, for example, the MLRO.
- A business relationship with a PEP or a PEP's family and close associates is subject to an increased level of formal review , for example, an increased frequency in the update of

customer due diligence information, or additional reviews where the customer requests a new service or product
- The account is marked or denoted as a PEP for ongoing monitoring purposes.
- Additional automated screening, such as imposing tighter thresholds for monitoring or more frequent monitoring.

Where a PEP is considered to be higher risk PEP, firms should consider more enhanced actions, such as:

- Taking more intrusive and exhaustive steps to establish the source of wealth and source of funds of PEPs, family members or known close associates of a PEP
- Oversight and approval of the relationship takes place at a more senior level of management, such as the Board.
- The relationship is subject to more frequent and thorough formal review as to whether the business relationship should be maintained
- Additional automated screening, such as imposing tighter thresholds for monitoring, or rules which are specifically tailored for PEP monitoring.

Payments to a PEP
Firms should be aware of the obligations under the Bribery Act to prevent bribery. On this basis, where a client is making a payment to a PEP, or to a state owned or controlled entity overseas, firms may wish to apply EDD on such transactions to ensure that they are not facilitating bribery. This may be achieved by utilising PEP screening on outbound payments, similar to the guidance provided in the above section on Sanctions Screening.

12. Transaction Monitoring

Ongoing monitoring of transactions should take place to ensure that transactions are in keeping with the clients expected KYC profile, and that the KYC Profile is in keeping with information available from public records. Firms should also consider the transactions carried out by its clients are in keeping with the expected commercial nature and purpose of the clients, such that transactions made by the client make commercial sense.

Firms should note that Transaction Monitoring obligations will not be met solely through the use of a Sanctions Screening and Negative Media searches. Firms should consider the volumes, values of transactions, frequency of such trades and the CDD profile and risk assessment of the firm.

Firms should consider the following elements, where these are relevant to the clients business model:

- Payments to countries or jurisdictions which are considered to be high risk, such as those identified by the EU or another relevant body as posing a high risk of money laundering
- Payments to tax havens of offshore secrecy locations.
- The total spend of a firm and its transaction patterns over an extended period of time is in excess of the clients profile or filed turnover.

- Transactions which are unusually high for a client of that type (e.g. a local sports club transaction high volumes with an overseas entity)
- Transactions which make no commercial sense for the client
- Transactions to beneficiaries which are not in the same industry, or which appear unconnected to the clients nature and purpose.
- Clients who are making an unusually large number of payments, or utilising a high number of currencies when compared to other clients
- Incidents where multiple clients appear to be paying the same overseas account for no justifiable reason.
- A high volume of cancelled trades, or trades which appear to have no commercial purpose (Return of funds to own account in same currency after a holding period)
- Repeat payments in the same day which may be aimed at avoiding thresholds (smurfing)
- New clients whose turnover is vastly in excess of other, similar clients.
- Transactions which are to Linked Individuals or shareholders, or to companies owned or controlled by the Persons of Significant Control, but which are not in keeping with the firms commercial purpose.

Monitoring may be automated or manual, however should be independent of those individuals who are involved in the processing and execution of trades in order to prevent a conflict of interest in which traders are able to supress alerts, or whereby they are incentivised to not report transactions owing to their own profits or remuneration.

A formalised process should be in place in which analysis is carried out on transactions on a regular basis which is capable of identifying the elements above.

A record or trail should be kept of those alerts which the screening system generated, and the process of investigation and review of those transactions including any evidence or additional materials which were gathered in order to clear those alerts.

13. Suspicious Activity Reporting

Firms must have in place a process whereby employees, officers and agents of the firm are able to report suspicious activity to the MLRO. The MLRO have a process whereby they are able to analyse SAR's which are received internally and to report these to the relevant authorities where appropriate.

Suspicious activity is any incident where an individual knows, suspects, or has reasonable grounds to suspect that a client, another employee or someone with which the business has a relationship is engaged in money laundering. Firms are required to ensure that they provide adequate training to their staff, such that individuals understand:

- What would constitute suspicious activity.
- Are aware of their obligations to report suspicious activity
- Are aware of the process for reporting such activities when they encounter it.
- Understand their obligations, post reporting.

AFEP best practice is to encourage "over-reporting" to the MLRO, such that the MLRO receives prompt and early disclosure of all events which they are able to make a decision on. Firms should avoid situations in which individuals are discouraged or prevented from making disclosures.

Firms should have a formal disclosure process, such as an internal SAR form, which can be submitted by the employee with relevant information about the nature of their submission and which allows the MLRO to investigate. Firms are however encouraged to allow informal reporting, but to log and track those reports through a formal process for record keeping procedures.

Firms should acknowledge the receipt of a SAR to the employee, reminding them of their obligations in regards to tipping Off, and also ensuring that they are aware of where to seek further help or guidance as required.

Firms should have in place a process for logging any internal SAR's which are received and for detailing the outcome of those reports, such that they are able to display and explain why a particular decision was made with regards to the handling of a SAR.

External Reporting of SAR's

Where a firm believes that an external report should be made, the firm should do this within a reasonable time frame.

Firms should familiarise themselves with the NCA's guidance on submitting better SAR's[8] As the guidance issued by the NCA is not industry specific, AFEP will not replicate the guidance here, however AFEP believes that firms should be aware of the benefits of well formatted SAR's and the advantages of submitting these reports to the NCA and would expect members to consider this guidance.

Defence SAR's (formerly Consent SAR's)
Firms should familiarise themselves with the new Defence Sar regime, its function, and the intention of this process. Firms are strongly encourages not to use the Defence SAR regime as a method of validating their clients, and should understand that a defence offered to a firm in relation to a client does not provide them with a defence or permission to continue trading with a client.

Firms are expected to understand the Defence SAR regime, and to have read relevant NCA guidance on this regime prior to utilising it.[9]

14. Training

Irrespective of the firms policies and procedures, a firm is only as good as the individual employees who apply those policies and procedures.

[8] https://nationalcrimeagency.gov.uk/who-we-are/publications/42-guidance-on-submitting-better-quality-sars/file
[9] https://nationalcrimeagency.gov.uk/who-we-are/publications/167-defence-against-money-laundering-daml-faq-may-2018/file

Employees who do not understand the requirements of those policies or procedures, or the implications of them, will weaken a firms overall defences against money laundering.

Firms should be aware that where an employee was not appropriately trained, firms may become liable for the failure of their employees in failing to spot money laundering.

Training should be risk based and proportionate to the staff and their role. Employees engaged in higher risk or AML specific roles, such as client onboarding, monitoring or oversight (the MLRO) are unlikely to be deemed sufficiently trained, by virtue of a 45 minute online training programme.

For this reason, firms should be able to demonstrate that they have training which is:

- Reviewed by the MLRO and has been deemed suitable for the firm.
- Is up to date and references modern laws and best practice.
- Relevant and specific to the firm, e.g. it contains examples and red flags which are appropriate for the firms products and risk profile.
- Is of sufficient depth and detail that employees know what they are required to do, and why.
- Contains a level of both Practical and Theoretical examples, such that employees know what the laws are and what they need to do, rather than concentrating heavily on legal structures and ramifications.
- Is appropriate to the role being performed by staff, for example staff in the Compliance team receive additional training or bespoke courses.
- Is able to test the knowledge and understanding of trainees and to record the results and completion of training.
- Informs employees of the consequences of their failure to identify and report any suspicious activity.

15. Good and Bad Practice Elements

Good Practice	Bad Practice
The firm has a clearly defined risk appetite which considers Product, Client, Delivery Channel and Geographic risk across the business	The firm has a single "product" risk assessment which covers multiple products, e.g. Payments, FX, Forwards, E-commerce platforms, Swaps etc are all considered to be one Product
The firm's product risk assessment is considered as part of the design of a new products	The firm's risk assessment does not specifically address the core risk elements, such as Customer, Geography, Product, as specific and distinct risks.
The firm's product risk assessment is consistent, documented and is clearly defined for each unique product.	The firm's risk assessment does not drive a change in behaviour, such as requiring EDD for

	users of high risk products or enhanced monitoring.
The product risk methodology is robust enough to identify risks, even when these risks are not something the firm currently has exposure to (e.g. cash handling)	The firm's risk assessment is not applied consistently across all products.
The firm is able to clearly articulate the risk they have considered and the methodology used for scoring those risks.	The firm's risk appetite cannot be tested or measured against specific risk elements, e.g. the firm cannot tell if it has a majority of high risk products.
The firm's risk assessment highlights key areas of risk which can be mitigated, such that products can be made to be lower risk if action is taken (For example by enhancing controls, increasing monitoring etc)	Assessments which fail to consider the funding sources, and the underlying risks associated with such payment methods (e.g. increased risk of fraud from certain card types or risks posed by acceptance of cheques)
The firm has a specific Risk Assessment for identifying and risk categorising PEP's where they have been identified.	The risk assessment considers, or is influenced, by factors such as revenue as during the risk assessment process.
	The firm's risk assessments are not linked to the board approved appetite
	A firms Transaction monitoring is based solely upon human/manual review by traders placing deals.
	Firms use a single training module for all employees, with no specific training for higher risk staff, or staff with specific compliance roles.