Lyddon
CONSULTING

+44 (0) 7979 132 341
enquiries @lyddonconsulting.com
www.lyddonconsulting.com

31st July 2023

The UK's financial services industry has invented for itself the right to use data providers to identify Politically Exposed Persons (PEPs)

Summary

The de-banking of Nigel Farage by Coutts/Natwest has shone a light on the regime in the financial industry for identifying PEPs. The industry claims the regime is an implementation of the laws for combatting Money Laundering and the Financing of Terrorism (known collectively as AML/CFT).

Only it isn't, in three important respects.

Firstly the UK financial industry has agreed with itself, through its own industry body, that it is entitled to 'place reliance' on lists supplied by a data vendor (typically through the World Check system provided by Refinitv) to identify PEPs. This right does not exist in applicable law.

Secondly the concept of the existence of 'lists of PEPs' is not grounded in applicable law. It is up to each institution to determine whether a customer is or is associated with a PEP.

Thirdly, and consequentially, the business process for identifying a PEP and then dealing with that determination has come to be significantly at odds with the one inferred by applicable law.

This reveals a defect in the formulation and implementation of applicable law in the UK which, while not the fault of the EU directly, has grown up around EU membership, where the formulation of Directives/Regulations and then their practical implementation is subject to the intervention of supplier lobby groups at various stages.

The outcome of that ranges from loopholes (like the one that enables payment scams), to the turning of legislation on its head (like the frustration of the law to cap credit and debit card fees), to in this case a group of suppliers awarding themselves rights that operate strongly in their favour.

A consideration at the next level is how financial technology (known for short as Fintech) has come to permeate the financial industry and not necessarily in a good way. A business opportunity has arisen for Fintechs out of the self-awarded expansion of suppliers' rights and the erroneous invention of the concept of 'lists of PEPs'. The result has been that the business process for PEPs has become built around the Fintechs' offering, suppressing the version that can be extrapolated out of applicable law.

This paper is in three parts:

1. using third parties to carry out AML/CFT work that is an obligation laid on an organization by law;
2. the erroneous concept of 'lists of PEPs'; and
3. what should a PEP process look like?

Overall conclusions are drawn at the end.

Part 1 – using third parties to carry out AML/CFT work that is an obligation laid on an organization by law

The right to use a data vendor to identify PEPs instead of doing the work yourself

Using a data vendor to identify PEPs is not supported in applicable law. Applicable law in this area has arisen from the original, global Financial Action Taskforce (FATF) Recommendations, through the 4th EU Anti-Money Laundering Directive (4AMLD) and into the UK's transposition of this Directive as The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (the MLRs).

The right to use a data vendor in relation to AML/CFT work has been introduced by a financial services industry body, called the Joint Anti-Money Laundering Steering Group (the JMLSG), in their implementation guidance, which has no status in law.

The JMLSG has no official status.

A financial institution or any other organization falling under the legislation may 'place reliance' on a third party for some AML/CFT work, but the right is limited to certain categories of third party, and the scope is limited to a very short list of tasks.

A data vendor is not a type of third-party on which financial institutions or any other organization falling under the legislation may 'place reliance'. This term means having the third party carry out work that the legislation says must be carried out, as an alternative to the organization doing the work entirely themselves.

In this document we have used the term 'obliged entity' for a financial institution or any other organization falling under the legislation. The MLRs use the term 'relevant person'.

Even if an obliged entity places reliance on the work of the third party, it remains responsible itself for the outcome.

Who can 'obliged entities' place reliance on?

'Obliged entities' can only place reliance on other 'obliged entities'. The types of 'obliged entity' are given in the FATF Recommendations, and repeated consistently in 4AMLD and the MLRs. Here is the listing from the MLRs, in which data vendors do not feature:

PART 2

Money Laundering and Terrorist Financing

CHAPTER 1

Application

Application

8.—(1) Parts 1 to 6 and 8 to 11 apply to the persons ("relevant persons") acting in the course of business carried on by them in the United Kingdom, who—

(a) are listed in paragraph (2); and

(b) do not come within the exclusions set out in regulation 15.

(2) The persons listed in this paragraph are—

(a) credit institutions;

(b) financial institutions;

(c) auditors, insolvency practitioners, external accountants and tax advisers;

(d) independent legal professionals;

(e) trust or company service providers;

(f) estate agents;

(g) high value dealers;

(h) casinos.

For what tasks can one 'obliged entity' place reliance on another?

An 'obliged entity' can place reliance on another 'obliged entity' only for a narrow range of tasks to do with Customer Due Diligence. These tasks are the letters (a) to (c) in FATF Recommendation 10, which map through to 4AMLD Article 13.1 and the MLRs Clause 28. Here is the 4AMLD rendition:

Article 13

1. Customer due diligence measures shall comprise:

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;

(c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

Tasks related to PEPs are not mentioned. Identifying the customer and verifying their identity is a business process step earlier on in the same business process that reveals whether the customer is a PEP or not, but they are not one and the same.

Interim conclusions

The business process steps relating to PEPs within the Customer Due Diligence process cannot be subject to 'reliance' at all. An 'obliged entity' is not permitted to have a third-party carry out that work, with the 'obliged entity' relying on the third-party's work.

Even if it was permitted for this work to be done by a third-party, a data vendor does not fall within any category of 'obliged entity'. One 'obliged entity' may only place reliance on another 'obliged entity' and not on any other type of third-party.

How has the usage of a data vendor become legitimised?

The financial services industry has formed its Joint Money Laundering Steering Group to deliver 'guidance' on the implementation of successive versions of AML/CFT legislation.

It re-issued its guidance upon the transposition of 4AMLD into UK law as the MLRs in 2017, under the following cover:

JMLSG

Prevention of
money laundering/
combating terrorist
financing

2017 REVISED VERSION

GUIDANCE FOR THE UK FINANCIAL SECTOR
PART I

June 2017 [Amended December 2017]

JMLSG's membership comprises the trade bodies for numerous sectors of the UK financial services industry:

Who are the members of JMLSG?

30. The members of JMLSG are:

Association of British Credit Unions (ABCUL)
Association of British Insurers (ABI)
Association for Financial Markets in Europe (AFME)
Association of Foreign Banks (AFB)
British Venture Capital Association (BVCA)
Building Societies Association (BSA)
Electronic Money Association (EMA)
European Values & Intermediaries Association (EVIA)
Finance & Leasing Association (FLA)
Futures Industry Association (FIA)
Investment Association (IA)
Personal Investment Management & Financial Advice Association (PIMFA)
Tax Incentivised Savings Association (TISA)
UK Finance (UKF)

In the first of the three books of guidance and under chapter 5 'Customer Die Diligence', JMLSG opined about the 'Nature of electronic checks' (5.3.46 – 5.3.50) and about 'Criteria for use of a provider of electronic verification of identity'.

Here are the clauses on the 'Nature of electronic checks':

Nature of electronic checks

5.3.46 A number of commercial organisations which access many data sources are accessible online by firms, and may provide firms with a composite and comprehensive level of electronic verification through a single interface. Such organisations use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a PEPs or sanctions list, or known criminality. Some of these sources are, however, only available to closed user groups.

5.3.47 Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Some electronic sources or digital identity schemes specify criteria-driven levels of authentication that are established through the accumulation of specific pieces of identity information.

5.3.48 Such information should include data from more robust sources - where an individual has to prove their identity, or address, in some way in

order to be included, as opposed to others where no such proof is required. The information maintained should be kept up to date, and the organisation's verification – or re-verification - of different aspects of it should not be older than an agreed period, set by the firm under its risk-based approach.

5.3.49 Negative information includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be necessary to mitigate against impersonation fraud.

5.3.50 For an electronic/digital 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 Register, or at a single point in time, is not normally enough on its own to verify identity.

It is notable that the phrase 'PEP lists' appears first here, without there being a precedent for it in the FATF Recommendations, 4AMLD or the MLRs.

There is no mention here of the limited extent to which an 'obliged entity' can have a third party discharge its tasks in the Customer Due Diligence process.

There is no mention of the status of a 'provider' not being that of an 'obliged entity'.

Here are the clauses for 'Criteria for use of a provider of electronic verification of identity':

Criteria for use of a provider of electronic verification of identity

5.3.51 Some commercial organisations providing electronic/digital verification are free-standing and set their own operating criteria, whilst others may be part of an association or arrangement which, in order to admit organisations to 'membership' require them to demonstrate that they meet certain published criteria – for example, in relation to data sources used, or recency of information - and carry out some form of checks on continuing compliance.

5.3.52 Before using a commercial organisation for electronic verification of identity, firms should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate, and independent of the customer. This judgement may be assisted by considering whether the identity provider meets the following criteria:

- it is recognised, through registration with the Information Commissioner's Office, to store personal data;
- unless it is on the Information Commissioner's list of credit reference agencies (see https://ico.org.uk/for-the-public/credit/), it is accredited, or certified, to offer the identity verification service through a governmental, industry or trade association process that involves meeting minimum published standards;
- it uses a range of multiple, positive information sources, including other activity history where appropriate, that can be called upon to link an applicant to both current and previous circumstances;
- it accesses negative information sources, such as databases relating to identity fraud and deceased persons;
- it accesses a wide range of alert data sources;
- its published standards, or those of the scheme under which it is accredited or certified, require its verified data or information to be kept up to date, or maintained within defined periods of re-verification;
- arrangements exist whereby the identity provider's continuing compliance with the minimum published standards is assessed; and

85

- it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.

5.3.53 In addition, a commercial organisation should have processes that allow the enquirer to capture and store the information they used to verify an identity.

JMLSG has wrongly united the PEP-related business process steps within the Customer Due Diligence process into the steps to identify and verify the identity of the customer. By doing this JMLSG makes it appear that these tasks are covered by the permissions contained the MLRs Clause 28 for obliged entities to place reliance on third-parties.

The word 'reliable' is used without clarification as to whether this means 'good for of placing reliance on their work for the purposes of MLRs Clause 39'.

There is an inference that the 'obliged entity' will carry out due diligence on the data provider, but there is no binding definition of what that due diligence should consist of, no requirement for proof that it was carried out, and no framework for adjudicating whether the due diligence was adequate at the beginning and upon periodic review. In fact there is no requirement for periodic review.

Instead there is the phrase that the information supplied by the provider 'is considered to be sufficiently extensive, reliable and accurate, and independent of the customer', and followed by a series of criteria for the provider to meet such that the making of their 'judgement may be assisted'.

This is not a robust control system even were the activity be permitted.

Conclusions on the impact of the JMLSG guidance

The JMLSG guidance represents a *de facto* endorsement to the members of the JMLSG members (who must constitute a dominant market position of financial services organizations in the UK) to use and place reliance on the work of data providers within their Customer Due Diligence processes, including for identifying supposed PEPs from 'PEP lists'.

The criteria for the selection of such a data provider are loose and not subject to corroboration, either at the outset or periodically. This is not acceptable, as the work consists of regulated tasks, which can have significant negative consequences for the subject person, and the tasks are being substantively carried out by an unregulated entity.

The attractions of this for the financial services organization are clear: automation and cost reduction. The working hypothesis must then be that the Customer Due Diligence process is built around data supplied by such providers (and there is no limitation to a single provider for all of what might be available).

If that is true, then the financial services organization has gone further than it is permitted to do in relying on the work of third parties for its Customer Due Diligence, and that it is relying on third parties falling outside the scope of eligibility for their work to be relied on by an 'obliged entity'.

The extent of unwarranted reliance goes beyond business process steps related to PEPs: it extends to the entire Customer Due Diligence process.

The JMLSG 'guidance' appears to have driven a coach and horses through applicable law, and permitted that any data from any source can be used in the Customer Due Diligence Process once the financial services organization has come to the point of considering the work of its provider(s) to be 'sufficiently extensive, reliable and accurate, and independent of the customer'.

The judgement of the financial services organization is taken to be infallible, and there is no provision for the applicant to challenge its results.

The result is a travesty of the original intentions of the FATF Recommendations.

Part 2: the erroneous concept of 'lists of PEPs'

There can be no such thing as a valid and reliable 'list of PEPs'.

The status of a person as a PEP or not is fluid. The categorization of a person as a PEP is not fully objective: it demands some element of subjective judgement.

There can be no self-certification, or certification by an 'authority' with which the person is in some way connected.

Having PEP status has only negative consequences. Getting a person onto a list of PEPs can be a form of harassment. The PEP process ought to be immune to the insertion into it of spurious data but it is not. Instead we learn that the UK has 90,000 PEPs and that 'obliged entities' rely on data providers.[1]

Several questions arise:

- What is the full list of data sources that these providers consult?
- Do people ever get crossed off this list, or is it only expanded, incrementally and possibly exponentially?
- Who has adjudged that this 'regulated activity' can be performed by an unregulated entity?
- Who is auditing the processes and controls of a data provider in performing what would be a 'regulated activity' were it undertaken by an 'obliged entity'?
- Is this another example of Fintech being employed in an area as if it was a panacea, with Fintech creating new detriments for every individual detriment that it claims to solve?

Identifying a PEP

In order to understand why there can be no valid and reliable list of PEPs, I propose to start with the section about identifying a PEP from a course I wrote for the Nelson Croom financial training company:

QUOTE

3.6.3 Video script - PEPs

An obliged entity has to take reasonable measures to identify PEPs who are themselves applicants or are connected to an applicant – but there is one big difference between how this plays out in practice and the UBO (Ultimate Beneficial Ownership) check.

This difference is that the obliged entity must screen everyone connected to the applicant for PEP status, whatever information the applicant itself supplies, and also whatever lists may have been issued by countries containing either (i) lists of positions in their country, the occupier of which would be considered as a PEP; (ii) specific lists of persons; or (iii) lists of persons with their positions.

Such lists risk being out-of-date, and may not include family members, friends or associates of a holder of a public office: family members, friends and associates are themselves considered as PEPs.

The definition of a PEP is not set in stone.

[1] https://www.thisismoney.co.uk/money/markets/article-12351619/Banks-shut-1-000-accounts-day.html?ico=mol_desktop_money-newtab&molReferrerUrl=https%3A%2F%2Fwww.dailymail.co.uk%2Fmoney%2Findex.html accessed on 30 July 2023

The criteria vary from country to country. It's a broad term and examples include:

- Senior political figures
- Senior executives within a government owned commercial company
- Senior government officials
- Senior members of law enforcement agencies
- Senior members of religious organisations.

Several further complications intervene, for example in the difference between a "Foreign PEP" and a "Domestic PEP".

Dealings by a bank with a "Foreign PEP" are deemed to be of a higher risk than dealings with a "Domestic PEP", on the basis that the "Foreign PEP" (e.g. a PEP from Canada applying for a bank account in France) is considered more likely to use a foreign bank account than a domestic one for illicit dealings: the Canadian PEP would in other words be less likely to want to receive the proceeds of those dealings into an account in Canada.

Another issue is the relative degree of exposure implicit in different levels of public office in a given country.

That issue comes down to the degree to which - according to studies and lists from FATF, Moneyval or similar organisations - the public processes in a given country are susceptible to bribery, corruption and other aberrations.

Then on top of that one has certain industry segments – identified by FATF, Moneyval or similar organisations - whose processes demonstrate a raised level of bribery, corruption and other aberrations. FATF documents refer to industries like defence procurement, oil&gas, and other primary resources.

The identification of a PEP will then lead on to a classification by degree of risk, denoted by the seniority of the public office involved, the country classification, the industry classification, and a measure of the perceived nearness of the public office to the factors of concern e.g. a regional official in a region in which primary resources are found might score as a higher risk than a senior government minister in the same country but whose portfolio was tourism or health.

PEP identification **is not** an exact science. Applicants can share who they believe, of all the natural persons connected to their business, would rank as PEPs but obliged entities will do their own searches and applicants need to be prepared for the bank to question what the applicant has presented and to supply extra information.

It would be good practice to already be in a position to assist the process by maintaining a register of all the natural legal persons connected to the business (Ultimate Beneficial Owners, shareholders, directors, mandators, operators) and having each one of them complete a PEP questionnaire, with any questions answered "yes" followed up and documented.

This may not stop an obliged entity wanting their own PEP questionnaire to be filled in, or the obliged entity identifying further persons connected to the business as potential PEPs.

Once a final list has been formed of the PEPs, each PEP will need to be put through the personal identification check (via passport, bank statement, utility bill etc.).

UNQUOTE

Key points deriving from the description above

An 'obliged entity' must carry out the work themselves. The classification by degree of risk does not lend itself to automation. There must be a degree of 'eyes on' evaluation.

By implication there is no such thing as a definitive, externally sourced list of PEPs that can be relied upon. FATF and Moneyval (the evaluation arm of FATF) do not issue lists of PEPs. National authorities issue lists of embargoed countries, and of sanctioned natural persons and non-natural legal persons. If a person is on such a list, it does not matter whether they also count as a PEP or not.

The EU issues a list of high-risk jurisdictions, but this is also unreliable as the efforts of countries to get themselves off the list can be considerable, and the list automatically classifies all EU member states as being low risk.

Where countries issue lists of their own supposed PEPs, these need to be treated with a high level of suspicion, as (i) the issuing country is often one where Moneyval has raised issues of susceptibility to financial crime and/or of weak AML/CFT controls in its financial system; and (ii) the list may fail to identify the extended network of agents and middlemen who, under the patronage of a PEP, handle the flows with which the PEP and their family do not wish to be associated legally or optically, only beneficially.

As there are no reliable lists of PEPs, there can be no valid test of the reliability of the data supplied by a data provider purporting to be able to deliver or support the identification of PEPs.

There is a danger that data from reliable sources like Moneyval (which is freely available anyway) gets blended with data from completely unreliable sources (like ancestry.com for identifying family members), and that the results are then treated as if their reliability was consistently on the level of Moneyval.

The process of data collection is susceptible to 'layering', a major risk in money laundering whereby money gets passed from one set of hands to another, gaining legitimacy incrementally along the way, until it comes out clean at the end. Ironically an equivalent danger exists in this area of combatting money laundering: unreliable underlying data becomes more credible as it rises up through layers of intermediaries, each one adding – thanks to its reputation, its widespread usage, or its apparently robust internal processes – an increment of believability: the result is 'data laundering', where the data itself is as unreliable as it was at the start, but it is now believed and treated as objective and official.

What appears to be happening in practice

A Fintech asking for a significant subscription charge for supplying 'obliged entities' with PEP-related information cannot just reproduce sanctions lists issued by national authorities. The lists must be extensive to justify the subscription charge. Commercial pressure takes its course and a long list is supplied.

The resulting list is not subjected to an 'eyes on' sanity check. A country like the UK, which has a low risk of public processes being susceptible to bribery, corruption and other aberrations, should have a commensurately small number of PEPs. With PEP status presenting a low risk, the status of being a family member or associate of a PEP presents an even lower risk.

The concern about a person having PEP status or not appears to have submerged the proper and due consideration of the risk that being a PEP presents to a financial services organization: that the person is more likely to be handling dirty money.

This connection appears to have been lost in the automation of PEP-related process within the UK financial services industry on the back of a capacious data feed from a Fintech.

Instead the industry's watchword appears to have become that, if data can be made available, it must be captured and processed, and the more data is available, the better. This mixture of belief in data and risk-aversion meets the technical capabilities of the Fintech and its need for revenues to deliver ever-expanding lists, whose veracity ceases to be questioned .

This becomes an industry in its own right and loses any connection to the purpose for which the status of PEP was formulated.

Part 3: what should a PEP process look like?

What should the PEP business process steps comprise?

The PEP business process starts at a fork in the road along the normal Customer Due Diligence business process: the fork is the step in the normal Customer Due Diligence business process to 'Establish whether the applicant is a PEP themselves (if a natural legal person) or has PEPs associated with them (whether the applicant is a natural or a non-natural legal person)'.

A positive answer automatically proceeds the application down the track 'Enhanced Due Diligence'. A negative answer allows the application to continue to proceed down the track 'normal Customer Due Diligence'.

The PEP business process in the context of 'Enhanced Due Diligence'

It might be helpful to characterise what 'Enhanced Due Diligence' is. It is not either (i) turning business away automatically; or (ii) terminating existing business relationships.

Here is the element on Enhanced Due Diligence (EDD) from the same Nelson Croom financial training course:

QUOTE

4.4.3 Video script - Practical instances of a situation where EDD is required

EDD is incredibly important because a failure to spot where it should be applied is a major process failure. Fines are levied by Financial Crime authorities for process failures as much as for the actual laundering of money. The fines are frequently out of all proportion to the amounts of money that passed through.

Cases that make the press do not stand out because the authorities appear stringent, but because it beggars belief that the obliged entity could have taken on the business without recognising a need for EDD.

This implies a culture at the obliged entity in which this one piece of business did not stand out, that questionable business was being taken on all the time: this one blew up but there was a lax AML/CFT culture and poor process and control. That is usually the judgement when a $100 million fine is imposed.

As we have seen, there is a 3-D matrix of where EDD should be applied, and its axes are Customer, Product/Channel and Geography. There is some overlap between Customer and Geography.

We have a cluster of "Customer" indicators that reflect the characteristics of "sunny places with shady people": legal entities with nominee shareholders or bearer shares, which are often shell companies or are personal asset-holding vehicles, and particularly complicated corporate structures with no obvious business rationale.

We have cash-intensive businesses.

Then we have the catch-all that the business is conducted in "unusual circumstances": what might be unusual in Denmark might be quite usual in Panama.

And finally we have the customer being resident in a "High Risk" geography; in practical terms this should be applied where the customer itself, its UBO(s), its connected PEPs, its directors, trustees and so on are nationals of or resident in a "High Risk" geography. The definition of "High Risk"

geography in 4AMLD knocks out sanctioned and embargoed countries and ones providing support for terrorism, but is more nuanced about others: obliged entities must rely on "credible sources".

In practice the EU has become its own credible source by engaging on a multi-year programme to analyse every country on the planet and determine whether it has corruption, criminality and/or a defective AML/CFT regime.

Finally we have the Product/Channel indicators and these lead with anything that restricts identification: not face-to-face, enabling anonymity, private, payments coming in or going to third-parties with no solid business rationale.

And there is a catch-all around anything new.

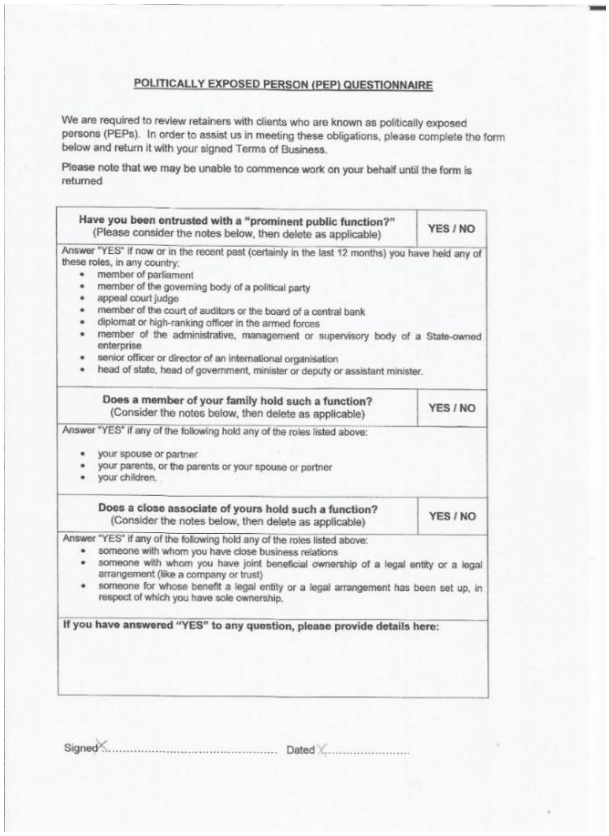
The one that should stand out is the simple statement of "private banking": then any obliged entity offering a wealth management or private banking service should put all their clients through EDD.

They may well do, but how many then get turned away? This is the really funny thing about EDD and in fact about the whole regime – there are multiple reasons for extra supervision and investigation but very few conclusive reasons to turn business away. Even Annex III of 4AMLD does not say, regarding countries providing support for terrorism, "turn the business away in all cases of a connection to such a country". Indeed, Annex III only deals with where the customer itself is in a "High Risk" geography: so an Iranian-owned company in Malta would not ring alarm bells because the customer would be the company, and Malta, being in the EU, is a priori Low Risk.

UNQUOTE

PEP business process and risk assessment

As stated, the PEP business process starts at a fork in the road along the normal Customer Due Diligence business process, and with a simple PEP Questionnaire like this one:



POLITICALLY EXPOSED PERSON (PEP) QUESTIONNAIRE

We are required to review retainers with clients who are known as politically exposed persons (PEPs). In order to assist us in meeting these obligations, please complete the form below and return it with your signed Terms of Business.

Please note that we may be unable to commence work on your behalf until the form is returned

Have you been entrusted with a "prominent public function?" (Please consider the notes below, then delete as applicable)	YES / NO
Answer "YES" if now or in the recent past (certainly in the last 12 months) you have held any of these roles, in any country: • member of parliament • member of the governing body of a political party • appeal court judge • member of the court of auditors or the board of a central bank • diplomat or high-ranking officer in the armed forces • member of the administrative, management or supervisory body of a State-owned enterprise • senior officer or director of an international organisation • head of state, head of government, minister or deputy or assistant minister.	
Does a member of your family hold such a function? (Consider the notes below, then delete as applicable)	YES / NO
Answer "YES" if any of the following hold any of the roles listed above: • your spouse or partner • your parents, or the parents or your spouse or partner • your children.	
Does a close associate of yours hold such a function? (Consider the notes below, then delete as applicable)	YES / NO
Answer "YES" if any of the following hold any of the roles listed above: • someone with whom you have close business relations • someone with whom you have joint beneficial ownership of a legal entity or a legal arrangement (like a company or trust) • someone for whose benefit a legal entity or a legal arrangement has been set up, in respect of which you have sole ownership.	
If you have answered "YES" to any question, please provide details here:	

Signed ..... Dated .....

This provides the necessary trigger to either continue with the normal Customer Due Diligence or to go into Enhanced Due Diligence. It is perfectly reasonable for 'obliged entities' to consult databases to verify this information as long as data protection regulations are adhered to, and as long as the objectives of the business process remain in clear view, namely to evaluate:

1. does the business relationship being proposed present a risk that the 'obliged entity' may become involved in the financing of terrorism or the handling of criminal proceeds?
2. If it does, how high is the risk and what reasonable measures can taken – over and above the measures embedded into the obliged entity's mainstream processes and controls – in order to monitor, manage and mitigate that risk?

There is no obligation to turn away business that involves PEPs, nor to terminate an existing relationship involving PEPs.

There is an obligation, however, if sanctioned or embargoed persons are involved, or if an existing relationship involves a person that is subsequently sanctioned or embargoed.

The issue is the threshold at which the risk is so high that the obliged entity cannot reasonably monitor, manage and mitigate the risk through the extra ongoing supervision that is the outcome of Enhanced Due Diligence's delivering a verdict of 'take the business on but apply appropriate risk management'.

That threshold is set by each obliged entity individually. It cannot be any other way, because the risk of failure – meaning that the obliged entity does become implicated in the financing of terrorism or embroiled in money laundering – falls on them alone and can result in high fines and even the loss of their permission to trade.

Conclusions on divergence between the PEP process inferred by applicable law and that based around reliance on a data provider

A PEP process based on reliance on lists compiled – or scraped from another source and uploaded – by a data provider mismatches what is inferred by applicable law. Lawgivers do not provide business process maps, but one can extrapolate from what is written that:

- Obliged entities should do the vast majority of the work themselves;
- They can consult undoubted external sources of data, with the bar set very high;
- They cannot place reliance on other obliged entities for PEP-related work, or on any other party;
- The business process is sequential and the PEP check should take place after the identification of the applicant and the verification of the applicant's identity – not all in one go.

Overall conclusions

Financial services organizations are not permitted to place reliance on third-parties for business process steps in the PEP process. Even if they were, the scope of parties upon which they may place reliance is limited to other obliged entities, and therefore excludes a data vendor.

The right to use a data vendor and to rely on it first pops up only in implementation guidance from a body with no status in law: the Guidance from the Joint Money Laundering Steering Group - an association of financial sector trade bodies with a dominant combined market share.

In other words the industry has self-gifted a series of very useful rights and remedies, replacing the need for them to do their own homework. This smacks of corner- and cost cutting, and has now delivered unjustifiable de-banking.

AML/CFT legislation was not meant to result in this. In this area, as in many others, the process of formulation of laws and their implementation appears to have severely malfunctioned. The role of Fintech recurs, as a panacea to deliver compliance in implementation at low cost, with the unintended consequence of introducing new detriments.

While the malfunction cannot be attributed solely to EU membership, there is a pattern whereby suppliers are able to influence the process at every level, with their influence probably being lowest on the Parliamentary process and the courts. In between – at the level of original formulation and then in implementation guidance – suppliers appear to be able to alter, frustrate, and reverse legislation at their discretion, and in the belief that they can escape sanction under legal process and/or from public regulators.

Public regulators in turn seem to suffer from ‘regulatory capture’ and to fail to exercise the rights and remedies conferred on them for the benefit of buyers. Buyers might rightly expect the regulator to lead a form of ‘class action’ against sellers, but the regulator either does not do this at all, or sets off another multi-year investigation process in which the sellers participate (and which they are able to steer), with the result that the detriments are not tackled.

This has been the case in financial services, for example, with payment scams (called Authorised Push Payment Fraud), high card payment fees (towards which the Interchange Fee Regulation might as well not exist), the right for non-bank payment companies to have bank accounts and services (towards which Article 105 of the Payment Services Regulations might as well not exist), and now de-banking of individuals (towards which clause 18 of the Payment Account Regulations on non-discrimination might as well not exist).

Invariably these situations involve quangos (like the Financial Conduct Authority and the Payment Systems Regulator), industry bodies (like UK Finance and Pay.UK), and detriment-specific working groups (like the APP scams steering group, and the Payment Strategy Forum workstream on access for non-bank payment companies), and then Fintechs looking to sell a service that supposedly mitigates the cost of implementation. This way-of-working has been a failure, and operated against the interests of buyers.

The de-banking of Nigel Farage is an example of such a failure in the processes of law-making and implementation in modern Britain.

BL/31.7.23