Call for Evidence: Review of the UK's AML/CTF Regulatory Regime

UK Finance is the collective voice for the banking and finance industry. Representing around 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

21 October 2021

Protecting the security, prosperity and reputation of the UK is a priority for the financial sector, which already spends billions each year to combat financial crime alone. Much of this resource is spent on low-value activity which has limited impact on disrupting illicit activity. In contrast, where resources are directed towards high-value activity, there is evidence that there is impact on tackling crime, reducing the impact of economic crime and its associated harms to society; limiting customer friction; and protecting the integrity of the UK financial system.

We welcome the ambition of this Call for Evidence (CfE) in reviewing the UK's Anti Money Laundering (AML) and Counter Terrorist Financing (CTF) regime. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Amendment Regulations 2019 (MLRs) have remained broadly static since they were first introduced in 2007. The MLRs do not fully reflect either regulated sector practice or the current ML/TF risks and threats in the UK today. They also do not reflect modern financial services activity, nor the public and private sectors' shared understanding of how economic crime risk enters and leaves the system. UK Finance welcomes the opportunity to respond to the CfE; our response is representative of our diverse membership and follows a series of member-led engagements.

The CfE is timely and provides an opportunity to consider solutions to address weaknesses within the AML/CTF regime against a backdrop of significant domestic and international reform. However, whilst we recognise the need to introduce parameters, the review of the regulatory regime should not be limited to a review of the MLRs, and should consider interdependencies or tensions between the MLRs and other legislation or guidance, such as the Proceeds of Crime Act (POCA), and the Payment Services Regulations (PSRs). A review of the UK's overall AML/CTF regime should consider all relevant regulations, legislation and guidance if it is to affect system wide reform and deliver more effective outcomes.

UK Finance supports the UK's approach that focuses on economic crime from a more holistic stance – as set out in the Economic Crime Plan (ECP). However, there is now a need for the legislative and regulatory framework to be updated in order to support and enable delivery of this approach. And supervisors, regulators, law enforcement and the private sector all have a responsibility to work together to deliver that framework.

In reviewing the regulatory and supervisory themes set out within this CfE, we have identified areas where the current AML/CTF regime could benefit from improvements. These key themes are woven throughout our response, and set out below:

- **The system needs a system leader in the public sector** – an issue identified in the Economic Crime Blueprint[1] - to address fragmentation and inefficiencies across the regime.

- **We need a better shared understanding of priorities and threats** - the system leader should oversee production of clearly articulated and actionable national threats and priorities, against which activity could be dialled up or down to remove inefficiencies in a fragmented ecosystem.

[1] The work commissioned by the Home Office on the delivery of the Economic Crime Plan.

- **The understanding of risk across the ecosystem needs to be enhanced** through a review of the existing regulatory perimeter by HMG, working with regulators, law enforcement and the regulated sector, to assess how risk enters and leaves the regulated sector and wider economy.

- **An effective AML/CTF regime must encourage the ability to switch off low-impact activity**, or at a minimum, dial up or down activity in line with threats in a manner endorsed by a system leader and recognised by supervisors. This would support articulated and actionable national threats and priorities, against which activity could be targeted, underpinned by key objectives.

- **We do not currently have a true risk-based approach but developing one is essential**. The systematic and acknowledged deficiencies in the UK's existing risk-based approach must be tackled to support high quality input for law enforcement. As a starting point, there needs to be recognition across all participants that a risk-based approach, by definition, accepts risk within the system. The potential crystallisation of risk, and even the actual crystallisation of risk, should be seen as the correct functioning of a risk-based approach where firms have applied reasonable and risk-based measures to address heightened risks and threat priorities.

- **There needs to be a more explicit focus on effectiveness and efficiency in both regulations and by supervisors.** A more effective UK AML/CTF regime, would reflect the principles of effectiveness promoted by FATF and presented through recent Wolfsberg statements.

- **Across the system, standards of supervision need to be strengthened.** Whilst the FCA is acknowledged as an overall powerful and effective regulator, other parts of the regulated sector are not supervised as effectively and therefore, the financial sector is expected to act as a de facto regulator of other regulated sectors. The regulatory perimeter needs to be better managed, to ensure members do not have to act as secondary gatekeepers to make up for these weaknesses

- **As well as strengthening supervision, the role of supervisors also has to evolve** to include a stronger focus on effectiveness, efficiency and competitiveness, and to provide more timely guidance. We recommend the creation of a formal mechanism where policy makers, supervisors and the private sector can address challenges at pace to help resolve thematic issues, such as challenges around access to banking or adopting new technology.

- **The scope of the MLRS needs to broaden to reflect those bringing risk into the system**. The principle should be regulating by activity and risk, as opposed to sector alone and it is crucial the regulatory perimeter is extended so those bringing ML/TF risk into the system are held to account. We repeat our arguments in the Economic Crime Levy (ECL) consultation response over the need to include sectors bringing fraud, and in turn money laundering risk, into the ecosystem

We recognise some of the suggestions above sit outside the scope of this CfE, but we believe that a wider look is needed at creating a more effective regime. Many of the proposals directly relate to topics in the CfE – namely effectiveness and efficiency, developing a robust risk-based approach (RBA) and the role of the supervisor.

All our members agree we should move towards a regime that has a true RBA with a strong focus on agreed threats and outcomes. Some members believe that in the longer-term, as we build a more sophisticated shared understanding of risk and threat, and can adjust resource accordingly, greater consideration should be given towards the desired outcomes of a system – in essence more of an outcome-based approach. However, there is also recognition that the first step before that can be considered is to improve the effectiveness and efficiency of the current regime.

The ability to focus activity towards high-impact activity is predicated on the delivery of a successful RBA, which the sector strongly supports. However, we do not believe that the UK has an effective RBA. We have included examples to support this view, both in our response and in the attached Annex A; these include a focus on theoretical risks instead of nuanced threats, disproportionate application of Enhanced Due Diligence (EDD) requirements, regulatory risk and other disincentives against the application of Simplified Due Diligence (SDD), and the rules-based content of the MLRs. The regime needs to truly provide comfort for the institutional application of a risk-based approach based on individual risk profiles to promote effectiveness and efficiency within the MLRs.

The supervisors also have an important role to play. A focus on whether firms have a control framework that complies with the MLRs, and whether their processes comply with that framework, will only result in effective outcomes if the MLRs are enablers of a true threat based, outcome focused, approach. Supervisors should therefore assess the effectiveness of a firm's AML/CTF framework through the lens of aggregate performance against shared, system-wide, objectives and threats – with a focus on outcomes. This is essential for firms to effectively reallocate resources from low impact activity to higher impact activity with demonstrably more effective outcomes.

Critically, an outcome based approach AML/CTF regime cannot simply be appended to the existing regime as another deliverable for the regulated sector. An output based regime can only work when regulators and supervisors promote a risk based approach based on intelligence-led threat priorities.

The focus on identifying low-impact activity within this review, is, in our view, in contrast to the proposals testing the introduction of low-impact obligations within the Statutory Instrument (SI) consultation, in particular through the proposed extension of beneficial ownership discrepancy reporting obligations. The government should consider assessing the effectiveness of the proposed updates to the MLRs contained within the SI, including the opportunity cost to firms, in line with the welcome focus on effectiveness within this Call for Evidence.

Companies House (CH) is a further example whereby the existing ecosystem across the UK's AML/CTF regime is weak, including inefficiencies and acting as entry points for risk into the system. Addressing these weaknesses to build a system where the regulated sector can rely on others to perform their own compliance obligations, will redirect significant resources towards system-wide efforts to cut crime and protect the integrity of the UK financial system. It is crucial that any reform proposals are considered holistically alongside those proposals being explored through CH reform, to avoid inadvertently introducing greater inefficiencies into the existing system.

Finally, we welcome again the ambition set out by HM Treasury across the scope of both this CfE and the SI. We appreciate the volume and complexity of some of the proposals explored within our response, and look forward to providing our full support with testing these further, as we move towards building a more effective regime that ultimately results in less dirty money flowing through the UK, and fewer victims of economic crime.

We are happy to discuss the content within this submission further. Please contact Aminah Samad at aminah.samad@ukfinance.org.uk with any questions.

1. What do you agree and disagree with in our approach to assessing effectiveness?

We agree with the proposed approach set out with regards to effectiveness, remaining aligned with FATF's established approach, while addressing common issues identified across previous reports. However, we believe the approach should go further and align with the principles articulated in the recent Wolfsberg paper on Effectiveness[2]:

[2] https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20Group_Demonstrating_%20Effectiveness_JUN21.pdf

- a focus on clearly articulated national priorities against which financial institutions can demonstrate risk-based control environments;
- where resources are appropriately allocated in a timely manner based, as far as possible, on live actionable intelligence and understanding of higher risk factors;
- where there are demonstrable positive outcomes from these controls, and a financial institution has the confidence to re-allocate resources from activity that delivers minimal risk mitigation to higher impact activity with demonstrably more effective outcomes without concern for regulatory criticism.

As the Wolfsberg paper notes, the aim of an effective system should be: *"Ultimately, each FI should be able to demonstrate effectiveness by telling its unique story, based on its risks and corresponding AML/CTF programme. An FI's effectiveness, as it relates to designated priorities or the AML/CTF programme overall, should be measured based on its compliance with law and regulations, how it is designed to provide highly useful information to government authorities in defined priority areas, and how the FI builds and maintains a reasonable and risk-based set of controls to mitigate the risks of the FI being used to facilitate illicit activity."*

Whilst the Wolfsberg principles were developed for financial institutions, we believe the core aims would be applicable to the wider regulated sector and would help rebalance the regime towards one that is more effective and efficient, both in use of resources but crucially on outcomes.

We also see access to banking as a cornerstone of an effective AML/CTF regime. Access to the regulated financial system not only provides consumers with essential protections but also assists law enforcement in accessing critical intelligence. As such, policy makers and regulators must design the identification and mitigation of unintended consequences, such as access to banking challenges and UK competitiveness, into the AML/CTF regime.

The CfE states it will not be recommending significant changes to the Proceeds of Crime Act (POCA) or other legislation such as the Payment Services Regulations 2017 (PSR 2017). We appreciate the need to focus the CfE, but members have to manage competing tensions between regulations, legislation and guidance. This includes managing risk whilst supporting access to banking or balancing sharing intelligence to understand threat with GDPR requirements.

If a core purpose of the MLRs is to help deliver high value intelligence to law enforcement, it is counterproductive to ignore interdependencies which impact where resources are directed. The MLRs are predicated on a risk-based approach, whereas POCA adopts an all-crimes approach which, as set out below, can tie up activity in low impact SARs reporting. We recommend the focus on effectiveness also considers consistency and cohesion across the wider regime.

The relationship between the PSRs and the MLRs needs to be explored given how risk enters and leaves the financial system. We, and law enforcement are increasingly seeing cashing out of the proceeds of fraud via crypto wallets or other means. However, there is currently no easy ability for members, law enforcement or regulators to systematically slow or halt payments to firms collectively viewed as high risk. Indeed, the pressure is to deliver ever faster payments – this needs to be balanced against appropriate powers to intervene where fraud risk is suspected.

As well as legal and regulatory alignment, supervisory standards across the board need to rise and the role of supervisors needs to evolve to include a more explicit focus on effectiveness, efficiency and competitiveness and helping support the regulated sector to manage thematic issues.

For example, well acknowledged challenges in some sectors, such as Money Service Bureaus (MSBs) mean our members end up expected to act as a de-facto secondary regulator to identify and manage risks with little regulatory guidance on the correct approach. Whilst we support a RBA, it is a failure of the system that there is no easy means for the public sector to help provide clarity on what an appropriate baseline should be, where, in effect, the risk has been handed off the risk for the financial sector to manage.

Currently there is no easy mechanism to get a supervisory steer on thematic concerns and tensions in the system. We recommend a formal mechanism to more easily and swiftly obtain a supervisory/policy steer on thematic issues or unintended consequences such as challenges around access to banking or adoption of new technology.

As below, work outside the MLRs review is needed on system leadership - the absence of which was identified as a gap in the Home Office Economic Crime Blueprint. An area we think should be in scope for a system leader includes producing a more developed threat assessment setting out priority areas and threats to allow firms to prioritise and devote resources towards high impact activity. This aligns with the National Strategic Priorities proposals.

The system leader should also have the ability, or drive mechanisms elsewhere for the system to proactively dial up or down activity, including the power to switch off low impact activity in the public and private sectors in a way that gives regulatory comfort. This would significantly support effectiveness and help firms reallocate resources towards areas of higher impact.

2. What particular areas, either in industry or supervision, should be focused on?

There are a number of areas of focus that we believe should be prioritised for discussions regarding the effectiveness of the UK's overall AML/CTF regime.

<u>Understanding the threat and system leadership</u>

We need an improved understanding of threat, setting out actionable threat priorities for the UK, and how those threats manifest as risk to firms within the regulated sector. We note that the National Risk Assessment (NRA) on Money Laundering and Terrorist Financing is not sufficiently detailed or granular to assess risks across the regulated sector for Levy purposes. The focus should be therefore to build upon the NRA and produce clearly articulated national threat priorities, aligned with the strategic priorities of the Economic Crime Plan. Setting out threats that are clearly targeted and rationalised, widely available to industry, which firms can design risk-based control environments against, would allow resources to be reallocated towards higher risk factors based on an agreed and shared evidence picture without concern for regulatory criticism. We cover this in more detail in Qs 9-11.

There is not currently a single public sector view across what is a fragmented ecosystem, nor the ability to resolve tensions with different parties focused on different areas and priorities.

A more effective regime would have a clear system leader, driving activity towards a defined outcome underneath which the objectives of the regime would sit (as set out in Q3.) As a priority, we believe consideration should be given to designing a system and system leadership which enables regulated entities to dial up or dial down activities to concentrate or reduce activities in line with threats.

<u>The legislative framework and scope of the risk perimeter</u>

Current legislation is often ineffective and inconsistent due to the existing system fragmentation, further complicated by falling across both the UK's reserved and devolved legislative framework. Longer term, there should be consideration towards how to introduce greater cohesion across all existing legislation, regulation and guidance, underpinned by core principles, such as enabling a true RBA, and supporting key objectives such as information and intelligence sharing. We acknowledge this is outside the scope of the CfE but believe it to be crucial.

Effectiveness also needs to consider the existing risk perimeter. Vulnerabilities in other sectors are exploited to enable scams bringing fraud and money laundering risk into the financial sector which cannot be effectively managed as the risk perimeter has now extended beyond their control. That creates inherent inefficiencies in the ecosystem. A harmonised strategy should focus on preventing economic crime through the inclusion of other sectors within the regime, not just financial institutions preventing or detecting laundering. There is a strong case for the scope of the MLRs to be extended to include identified sectors bringing risk into the system including social media, telecommunication companies, ISPS and marketplaces. We set this out at Annex B.

We note, it will not always be appropriate to extend the full application of the MLRs to new sectors, particularly when considering customer impacts and competition but believe there should be a minimum a set of obligations to prevent acting as a catalyst for fraud and money laundering risk.

There should be the ability to move quickly as criminals adapt and exploit weaknesses. This could be, (a) flexibility within secondary legislation to bring types of activity and/or sectors into scope of the MLRs; (b) the ability for a system leader to require reporting on types of activity where there is strong intelligence suggesting exploitation or (c) a combination of both. As above, crypto assets outside the MLRs are being exploited for cashing out proceeds of fraud but there is no mechanism to direct these crypto assets to report risk. The system only allows for case by case reports to be made under the SARs regime but there is a need for strategic reporting so that early proactive efforts can be made to identify and apply controls towards relevant threats, thus reducing ongoing issues and displacement of risk throughout the ecosystem.

<u>Supervision and Gatekeepers</u>

Building a system where there can be greater reliance within the regulated sector on other regulated firm's compliance would go a long way to deliver a more effective regime. This requires a focus on both supervisors and gatekeepers such as CH.

The lack of consistency of approach and effectiveness across supervisors encourages inefficiencies and introduces unnecessary risks into the system and raising standards would help ensure those bringing risk into the system are held accountable. Addressing this needs adequate standards in places across all supervisors, underpinned by a common set of guidelines and principles as to approach. We cover this in more depth at Q52-55.

Inefficiencies are also inherently inbuilt given the inability to rely on work undertaken by other key areas of the regime such as the use of CH data. It is crucial that entry points such as CH are robust to prevent abuse and to avoid duplication of work and unnecessary costs. It also underpins the success of initiatives such as Digital ID and is more pressing given the proposed Levy spend on CH reform. We discuss CH Reform in more depth at Q3 and within our SI response.

<u>The Risk-Based Approach</u>

A RBA, by definition, should accept risk within the system and see potential or even actual crystallisation of risk as the correct functioning of a RBA - as long as firms have applied reasonable and risk-based measures to address priority risks and threats. System efficiency and effectiveness is predicated on the existence of a successful RBA which supports flexing of resources and activity.

As above, supervisors should therefore assess the effectiveness of a firm's AML/CTF framework through the lens of aggregate performance against shared, system-wide, objectives and threats, allowing firms to effectively reallocate resources from low impact activity that delivers minimal risk mitigation to higher value activity with demonstrably more effective outcomes.

Critically, an outcome-based approach AML/CTF regime cannot simply be appended to the existing regime as another deliverable for the regulated sector. An output-based regime can only work when regulators and supervisors promote a risk-based approach based on intelligence-led threat priorities.

We strongly believe the current RBA is not working effectively or as intended, and discuss this in depth at Q19.

3. Are the objectives set out above the correct ones for the MLRs?

The objectives set out in the CfE would all seem, in the case of the reporting obligations, the role of supervisors and the shared work on understanding threat, sensible outputs of an effective regime. However, we do not believe they should be the primary or only objectives or outputs, and as below we have concerns on the objective on Beneficial Ownership (BO).

There needs to be clarity on how any overarching objectives for the MLRs would sit and align with Strategic National Priorities and other requirements such as POCA obligations or the NRA. Otherwise, it could add further complexity and confusion to the system, particularly if it was not clear which objectives or priorities had more weight or what view regulators would take.

The wording of the primary objective, "the regulated sector act to identify, prevent and report suspicious transactions" is limited in scope and not equally applicable across all the regulated sectors. We instead suggest "the regulated sector acts to identify, prevent and report ML/TF."

There are notable gaps such as no reference for supervisors to support effectiveness or competitiveness. It is also surprising there is no mention of customers given challenges around access to banking for some customers and business where the costs of compliance would outweigh the commercial drivers, and/or there is a lack of effective supervision elsewhere. We suggest access to banking needs to be a key pillar of an effectiveness-based AML/CTF regime (given that the alternative is shadow banking/hawala and resultant loss of transparency) and helping resolve tensions on this should also be reflected in the objectives of supervisors.

Although we support the objective of preventing the exploitation of UK corporate vehicles and other forms of legal personality, we strongly disagree with any extension of discrepancy reporting without a full cost-benefit analysis, and in the absence of a clear AML/CTF strategy incorporating CH reform believe that:

a) Any measures to ensure accurate and up-to-date BO information are designed to deliver against this objective in an effective and proportionate manner; and
b) The burden of ensuring accurate and up-to-date BO information should fall on UK companies themselves, with effective public private collaboration to identify discrepancies within the data based on threat typologies.

More robust initial checks by CH and ongoing data analysis - a 'check it once' approach supported, as opposed to conducted, by the regulated sector, driving significant efficiencies in preventing abuse and reducing costs across the entire regulated sector. It would be a strange outcome of the ECL for the regulated sector to contribute funding towards strengthening CH but not be able to sufficiently rely upon the CH checks and have to replicate the same checks every time a firm establishes a new business relationship.

There is a key role for registered entities to keep their own BO information up to date as per obligations to do so under both the MLRs and CH rules. In addition, it is the obligation of directors to update CH information as part of strengthening the gateways and levelling up standards. Companies are also under a legal obligation in the MLRs to inform their bank of relevant changes. However, there is no enforcement for companies that fail to do this.

National BO registers are not the only way to improve transparency of ownership and do not address companies established overseas. Property ownership and public procurement are two examples where alternative public administration requirements can improve transparency (e.g. through robust disclosure, central registration, pre-qualification and screening procedures). Greater public sector data sharing can also support a risk-based approach through more effective risk assessment and network mapping of UK and overseas companies.

An alternative approach, in line with proposals on system leadership is to set out strategic objectives for the entire regime, accompanied by clarity on what outputs are needed to support these objectives and what outcomes this should deliver.

For example, objectives for our members should achieve material prevention, detection and reporting for the benefit of the financial system and those who use it, and not to focus on technical compliance or activities that do not meaningfully change the dial. This would provide the overall system with a shared purpose, ideally underpinned by shared governance, underneath which the suggested primary and secondary objectives suggested in the CfE would sit.

We also note that any overall objectives should be measurable in order to regularly assess the effectiveness of the regime as a whole, with public and private sectors collaborating under the oversight of a system leader to address emerging threats, weaknesses in the regime and any unintended consequences at pace.

We would welcome supporting consideration of such an approach further as if done correctly, it would provide a holistic framework for prioritisation of activity aligned to threat, all underpinned by an enabling legal and regulatory framework where all parties are clear of expectations.

4. Do you have any evidence of where the current MLRs have contributed or prevented the achievement of these objectives?

We believe this question is addressed through our responses to the sections on high and low impact activity, as well as the later evaluation of the existing RBA.

We reiterate concerns with the third primary objective, and strongly disagree it is the role of the MLRs to set out the rules applicable to CH. We also believe the lack of explicit focus on effectiveness and efficiency, or competitiveness has exacerbated tensions between managing risk and access to banking that it is not appropriate for the financial sector to manage alone.

5. What activity required by the MLRs should be considered high impact?

There is no definition of ‘high impact activity’ but whether activity is high impact should be judged on how effectively it delivers against any future overall regime objectives. Depending on the articulation of these high impact activity, there may be activity that effectively manages a firm’s money laundering risk and results in highly useful information being submitted to law enforcement.

Currently, we consider correspondent banking provisions to be broadly helpful, albeit principal to principal activity could be excluded explicitly as manageable on the basis of customer risk rather than the automatic application of EDD (as opposed to through vague "involving the execution of payments" language). More detail is at Annex A.

Outside of the MLRs, we welcome the recent approach taken to revising JMLSG guidance on Transaction Monitoring (TM) in an effort to encourage focus on higher risk TM alerts. We hope this formal recognition of the need for a nuanced view in existing guidance to encourage high impact activity should continue across the board.

Ultimately, the areas that members consider as truly high impact on tackling money laundering and improving controls on financial crime risk management are less the mandatory requirements under the MLRs and more discretionary activity focused on public private partnerships such as supporting the Joint Money Laundering Intelligence Taskforce (JMLIT).

JMLIT is viewed as supporting high impact activity across the ecosystem by the provision of intelligence regarding emerging threats and risks shared between the public and private sectors, in turn allowing a better understanding of risks across the sector. We encourage the further development of this kind of public private partnership. To increase the benefits, the intelligence shared through JMLIT should be more widely communicated across the regulated sector.

6. What examples can you share of how those high impact activities have contributed to the overarching objectives for the system?

The examples above seem aligned with the EEC commitment to improve the effectiveness and efficiency of the whole system in response to economic crime, increasing high impact intelligence and reducing low impact activity that delivers little benefit.

To build on this, we require improved feedback from law enforcement to help define more formally what constitutes "high impact" activity or "high value" reporting. The ambition of the SAR’s programme, focussed on uplifting capabilities to deliver enhanced analysis and improved intelligence outcomes, is welcome. However, this is still under way and needs progress on a wider range of legislative and non-legislative proposals, particularly around Defence Against Money Laundering (DAML) and SAR reporting, including the ability to switch off low impact reporting.

7. Are there any high impact activities not currently required by the MLRs that should be?

As above, one of the most impactful introductions to the existing regime would be a mechanism to more easily stop or vary activity and reporting in line with existing threats. Being able to work towards these priorities and outcomes would allow the flexibility to resource high impact activities, strengthen the overall regime and provide highly useful information to law enforcement.

We also believe the MLRs, whilst technology neutral, could benefit from clearer rules for designing and implementing new technologies and the standards any new system should meet.

Other areas where firms would support increased focus are on fraud, as there is not currently sufficient means to protect customers from online scams within the Online Safety Bill. We believe these sectors should be brought in scope of the MLRs. We also believe the MLRs should encompass means to tackle fraud risk by providing greater regulatory protections to firms to slow/delay or block individual payments (where they are not yet the proceeds of crime) and for a system leader/regulator to be able to require a halt/delay on transactions to certain high-risk recipients until fraud risk is addressed.

8. What activity required by the MLRs should be considered low impact and why?

In responding to this question, we would first make some general observations.

Again, there is no definition of 'low impact' activity but ultimately assessing if activity is low impact should be judged on how effectively it delivers against any overall regime objectives. In that case, low impact activity may be activity that never or rarely reduces economic crime risk.

However, members welcome the focus on low impact in the CfE. The view is that much of the current financial crime prevention activity is low impact and that demands are increasingly additive for little outcomes and undermine our ability to compete internationally. It also results in opportunity cost of significant resources that could be better put towards high impact activity. A 2021 report by LexisNexis assessed the annual cost of AML compliance by financial institutions as amounting to £28.7bn in the UK. One large member spends over £500m per annum on tackling financial crime alone - equivalent to their annual cost of running their branch network.

Low impact activity is driven by a number of factors, but primarily lack of a true RBA in regulation and therefore in supervisory expectation. Due to the absence of defined threat priorities and of a clear objective for the AML/CTF regime that the outcome of controls can be measured against, regulation and supervision is in practice more process driven than outcome focused. Prescriptive regulations will, in the absence of a clearly articulated objective, inevitably result in low impact regulatory burdens and reduces the ability to focus on new and existing higher risk threats. We cover this in more detail below.

Another driver is that transposition of mandatory EDD and other rules-based measures from the Money Laundering Directives (MLD) without a stated policy objective other than transposition has resulted in a lack of clarity in a number of areas. Examples include the requirement to take reasonable measures to determine and verify the "*law to which the body corporate is subject and its constitution"* (Reg. 27.2) and subsidiaries and branches of UK firms applying "*measures equivalent to those required by these Regulations*" (Reg 20.3). Ambiguity drives low impact activity because firms have to invest resource to reach a defensible position.

Whilst firms do not wish to focus on low impact activity, the approach to AML controls will be driven by four things: legislation and regulations; supervisory approach and expectations; guidance issued by authoritative bodies; and firms' risk appetites. As elsewhere on domestic PEPs and MSBs, steers (or the absence of clarity) from the supervisor will send very powerful signals, and in the absence of detailed guidance directing otherwise, can lead to significant compliance irrespective of risk. It cannot be a coincidence that the majority of firms, who elsewhere have different risk appetites, have overwhelmingly taken similar approaches to certain cohorts of client that are otherwise legitimate but as a sector pose additional risk (for example, as identified by the NRA). This is a good starting point for identifying areas of low impact activity.

Therefore, in tackling low impact activity, as well as requirements on the regulated sector, a more effective approach would see formal adoption of the FATF principles on RBA and supervision into the regulations. This would ensure supervisors better support the regulated sector to deliver improved outcomes.

Whilst we welcome the ambition of the CfE, many large UK institutions have headquarters in other EU jurisdictions, so there is the risk that elements of the EU consultation, which would introduce a range of new mandatory and arguably not risk-based elements could trickle down to UK institutions. To avoid either creating divergence or secondary gold-plating, the UK should work with other jurisdictions to promote the benefits of a truly public-private, RBA.

We set out at Annex A, examples of low impact activity, summarising some below, and have covered CH discrepancy reporting (which we see as a strong example) above. We note in principle a number of these activities should be examples of high impact activity, such as TM and EDD. However, due to the barriers set out, in practice, these have become examples of low impact activity.

Customer Due Diligence

There are customers and activity where the level of Due Diligence expected is disproportionate to the activity or actual risk, and where a more calibrated approach in legislation and regulation would allow resources to be better focused. An example is changes to Pooled Client Accounts (PCA) in the 4th MLRs. The absence of operationally viable Due Diligence when a customer is not low risk, has resulted in excessive compliance for little benefit and increased challenges on access to banking, even for firms that themselves are within scope of the MLRs.

The same applies to customer reviews where the MLRs and guidance should be more explicitly event driven, as opposed to periodic, customer reviews following a risk-based approach. This would help the sector better free up resources to reallocate towards higher risk activity – strengthening the ability to detect money laundering and keep risk out of the financial system. Equally, reducing low impact Due Diligence is not only important from managing financial crime risk, but in helping ensure access to banking.

The inability to get good faith protections from regulators (or other protection in guidance) means there is little incentive to carry any risk where the commercial benefits are low. Addressing this requires steps to both increase risk appetite and reduce the cost of compliance to facilitate access more easily to banking for clients where the risk reward ratio is currently imbalanced.

Mandatory Enhanced Due Diligence (EDD)

EDD can be a powerful tool to manage risk, but mandatory EDD measures in a range of areas can be counterproductive resulting in even low risk clients being subject to excessive compliance. Areas we recommend a different approach include High Risk Third Countries (HRTC) (Q.30) and PEPs, where allowing greater differentiation to include appropriate calibration towards domestic and non-domestic PEPs (in line with FATF r.12) would help reduce low impact activity. Further detail is set out in Annex A.

Clear expectations on correspondent banking and where there can be reliance on supervisor approval of a firm would be a great step forward. Whilst mandatory EDD required under Reg. 34 does not apply to intra-UK correspondent banking relationships currently we have firms who are heavily regulated and supervised by the FCA exchanging large amounts of information to

demonstrate compliance as opposed to reduce risk. Members also believe that mandatory EDD on correspondent trading (principal to principal) introduced by the MLD is disproportionate and low impact.

Transaction Monitoring

This is one of the areas of greatest cost, and arguably where the return in terms of outcomes is lowest. It also illustrates the power of regulatory expectations. Whilst there is no legislative or regulatory requirement to investigate every single TM alert, the view of the sector is that there is a clear supervisory expectation to do so.

If a firm does not investigate a low-risk TM alert as resource has been allocated onto perceived higher risk investigations, and it later transpires that money laundering has occurred that would have been flagged by the TM alert, then the view is they will face regulator action, even if it was the right decision at the time to make on an RBA.

This means many firms take a conservative approach to TM systems, often running false positive rates in excess of 90-95%. One firm noted the existence of transaction monitoring rules with SAR conversion rates of less than 1000/1, with FTE staff dedicated to reviewing these. This becomes hardwired given the lack of guidance or regulatory comfort to support recalibrating systems or switching off old systems to move to newer systems. Further complexity is added when considering the management and customisation of TM scenarios required under different regulatory regimes across the EMEA jurisdictions. This is why members welcome the proposed draft amendments to JMLSG as a positive outcome of the ECP.

The current absence of approved guiding principles means the default is a cautious resource intensive approach driven by the need to demonstrate controls to regulators as opposed to effective management of risk. This also reduces the ability of the financial sector to detect or monitor risk due to the level of activity needed to handle the noise in the system.

The opportunity cost is significant – there are an estimated 20 million TM alerts per year of which 8.5 million receive a Level 2 investigation. This ultimately leads to around 500,000 SARs a year to the NCA – a conversion rate of 2.5% - and there is again a shared view that the large majority of these SARs add little value to either the public or private sector in terms of detecting risk.

This all involves considerable resource – on a conservative estimate of an average of 30 minutes per TM alert, that is 10 million hours or nearly 5,000 FTE of resource. To put that in context, that nearly as many FTE as the NCA and on the conversion rate, of that 5,000, only 125 FTE would be working alerts that lead to SARs. Whilst these are only approximate calculations, they demonstrate the extent of sunk costs in just one part of the system.

This is why, as below, we believe there needs to be a fundamental reset on TM reporting – with far better direction on targeting, with more regulatory and industry guidance on what ‘good looks like’ to give firms the confidence to reprioritise resource to higher impact activity.

As an example, reallocation of resources towards high impact activity could include a focus on the points below to help provide higher quality intelligence to law enforcement.

- Further work to refine TM rules and better target them to take account of the business activity/ products/ services of each legal entity/branch.

- Mapping of typologies to products/services and building further targeted rules around emerging typologies.
- Developing further targeted product/service training to the 1LOD that focuses on how products/services may be exploited for money laundering or financial crimes.
- Investing in network analysis technology.
- Engaging in JMLIT and other public-private partnerships and other activities to improve our knowledge of the external threat environment.

As part of a wider look at effectiveness and efficiency it is worth exploring if and how the MLRs (perhaps underpinned by the powers of a system leader) could support sharing of TM alerts across the sector, and perhaps even with law enforcement, to ensure better calibration of activity and more sophisticated data mining. This is also a potential use case for the New Payments System.

Defence Against Money Laundering (DAML) SARs

The inflexibility of the MLRs and the SARs regime is highlighted by DAML SARs – the most resource intensive types of SARs for public and private sector – that are low impact. An example is the lack of legal ability for UK firms to safely conduct business activity in relation to cannabis lawfully produced in other jurisdictions for recreational purposes– the 'Canadian cannabis' issue.

This is both anti-growth, as many firms have now moved their engagement on what is a multibillion-dollar business to other jurisdictions, but equally still creates significant compliance to ensure that firms are not directly or indirectly dealing with a business involved or profiting from this legitimate activity (such as a cardboard manufacturer making boxes for the distribution of lawfully produced recreational cannabis). Not only is this significant compliance activity and costs for little benefit, but often leads to a DAML SAR which is of little use to law enforcement.

There is a need for a wider look at the DAML regime, now nearly 20 years old to reflect how it can be applied to how financial transaction operate now, but those are points for the Home Office and industry to consider as part of the SARs reform programme.

9. Would it improve effectiveness by helping increase high impact, and reduce low impact activity if HMG published Strategic National Priorities AML/CTF priorities?

As above, there is a lack of a consistent public sector view on threats and priorities that can be used to allocate resource and navigate legal and regulatory tensions.

There are differences on the best way to achieve this view. Some members believe it preferable to expand the existing NRA to focus on all economic crime, rather than introduce additional new priorities. This would be aligned with the proposal to consider broader Economic Crime Regulations, building out from the MLRs, with requirements for different sectors depending on the type of risk.

All members agree the existing NRA could be enhanced, particularly by ensuring it contains an adequate level of granularity and specificity to assist regulated sectors in responding to specific threats. It was also noted during the consultation of the 2020 NRA, the private sector had four weeks to provide feedback across a breadth of risk and sector types. Whilst the impact of Covid was understandable, this was not sufficient to explore or feedback upon such a complex area.

Other members believe Strategic National Priorities would be a useful addition to a more granular NRA if they do not introduce additional responsibilities that must be complied with in addition to

current priorities/ crimes, but allow existing resource and focus to be flexed. They would need to be sufficiently focused to offer a genuine steer rather than list all economic crime types.

If there are Strategic National Priorities, it is vital that the private sector is properly involved in the process and is clear on the expectations and outcomes of their existence. They would need to be updated on a regular basis, (at least annually) due to the dynamic nature of threat evolution. There also needs to be the means to support application of any increased granular intelligence so members believe that the proposed system leader would be important to maximise their impact.

Whether introduced or not, Strategic National Priorities and/or the NRA must be supported by increased granular, underlying sharing of public-private intelligence. As both Strategic National Priorities and the NRA are likely to be issued relatively infrequently, real value is derived from continued JMLIT activity, potentially including expansion to new sectors, changes to legislation enabling the sharing of valuable intelligence at an earlier stage, and data sharing projects.

10. What benefits would Strategic National Priorities offer above and beyond the existing National Risk Assessment of ML/TF?

This is in part linked to the future of the NRA but as a principle, members believe a means to help firms better identify and mitigate risk is welcome if it allows targeting of specialist resource to focus on “high impact” activity and the disruption of economic crime.

Some members believe that gaps exist on ML/TF; for example, the NRA acknowledges that fraud and tax evasion are the most common crimes but the risk is not formally assessed in a similar manner to ML/TF. The NRA also overly focuses on retail banking activities, and does not necessarily recognise or make distinctions for wholesale or capital market sectors.

If Strategic National Priorities were accordingly broad, in a similar way to those produced by FinCen and were explicitly produced to support focusing activity and resources towards agreed priorities/threats, they could be more effective in terms of outcomes. If used in this way, Strategic National Priorities could enable an agile, prompt, risk-based and intelligence- led approach, and reflect future priorities, whereas the NRA has traditionally been focused on past data.

Getting this right would allow industry and the public sector to direct scarce resources to focus on the “high impact” activity and greater disruption of financial crime. Again, robust public-private partnership would be welcomed to achieve this common objective.

Whilst members support the May ECP Statement of Progress and the 7 areas of public private partnership priorities we now need to make operational material changes to the ML regime in a similar manner to the US FinCen Reforms, where FinCen published both priorities and a definition of effectiveness and efficiency.

If considering the approach taken by FinCen, the scope of the Strategic National Priorities and/or the NRA would need to expand as above. Whilst this would be welcomed by industry, it could prove to be a significant challenge to HMG as all supervisors and supporting legislation could require guidance, similar to the JMLSG model for ML/TF. We cover this issue in more depth at Q50.

We do not underestimate the challenges and whilst the US model, alongside others, is a useful benchmark, members believe maximising the UK’s Economic Crime framework would allow a more integrated approach than the US. We would welcome further discussion as there are real gains here.

11. What are the potential risks or downsides respondents see to publishing national priorities? How might firms and supervisors be required to respond to these priorities?

The EECP already sets out strategic priorities on economic crime. It would be useful to understand more about how Strategic National Priorities would differ to these.

Revised Strategic National Priorities beyond existing requirements could add further layers of complexity and without removing low impact activity create additional requirements for little benefit. Critically, a threat-focused AML/CTF regime cannot simply be appended to the existing regime as another deliverable for the regulated sector. A more output based regime can only work when regulators and supervisors focus on a true RBA and intelligence-led approach.

There needs to be recognition of the potential for criminals to adapt and for risk to be displaced elsewhere within or outside the system so there needs to be the ability to bring other sectors and activity within scope quickly. We have seen how fraudsters adapted to the introduction of Confirmation of Payee.

Ultimately Strategic National Priorities will only be effective if they are accompanied by the appropriate means to update frequently and ensure that activity can be flexibly dialled up or down.

12. What evidence should we consider as we evaluate whether the sectors or subsectors listed above should be considered for inclusion or exclusion from the regulated sector?

Our starting point is that we need an AML/CTF regime proportionate to the risk, designed to mitigate the threat and suitably dynamic.

On the sectors listed, we note the Gambling Commission's annual Money Laundering and Terrorist Financing Risk Assessment identified Adult Gaming Centres, Bingo (Non-Remote) and Betting (Non-Remote & On-Course) as 'medium risk' from a money laundering perspective, with Betting (Non-remote & Off-course), Remote & Non-Remote Casinos, more Betting and Bingo) as 'high risk'. It will be for HMT to decide if based on this, they should be considered for inclusion under the MLRs.

Equally, some members wonder if further guidance may be required on the antiquities sector as there is external evidence that denotes the antiques industry as vulnerable to terrorist financing due to illicit sales of stolen antiquities and cultural artefacts.[3]

13. Are there any sectors or sub-sectors not listed above that should be considered for inclusion or exclusion from the regulated sector?

We repeat the call in the ECL consultation (at Annex B) for other sectors who bring fraud and in turn money laundering risk into the system to be brought within the scope of the MLRs. There is also a wider point if the time is now appropriate for HMG to consider the prospect of Economic Crime Regulations with responsibilities and duties designated to applicable sectors.

In considering other sectors, crowdfunding was recently identified as a sector of interest under the EBA consultation on technical standards on crowdfunding service providers in June 2021 and some members have identified potential risks in this space. Crowdfunding platforms allow a wide range of

[3] The FATF's 2015 Report on Financing of the Terrorist Organisation Islamic State in Iraq and the Levant

investors to support projects requiring funding, with attractive returns, but present higher risk for lenders as these services are under less direct regulatory scrutiny than MLR regulated entities. The global nature and the relatively high volumes of lending opportunities mean organisations are less likely to be able to conduct adequate CDD. This permits legitimate funds being channelled into fraudulent or mis-sold investments, or the use of legitimate projects as money-laundering vehicles.

Other members believe traders of luxury goods should be included within the scope of the MLRs, or at the very least be subject to targeted CDD obligations and Source of Funds checks above defined thresholds, for example, where single transactions to personal customers exceed value X, or through any payment methods of linked transactions that exceed value Y, through any payment method. Whilst a definition of luxury goods may be difficult to formulate, there are obvious ML risks associated with certain high-end transactions, as evidenced by recent UWO cases.

On the other hand, the regulatory perimeter can drive low impact activity, for example, the inability to rely on KYC of other regulated firms, or to easily offer PCAs without significant compliance activity. We set out in the SI Consultation our thoughts on proposals to descope, or at the least recalibrate requirements on AISPs because whilst regulated, they are low risk activities.

Another subsector to be considered for exclusion relates to international offices of the non-profit sector, where activity is low risk. If a donation is made to an overseas subsidiary of a regulated UK firm which is a charity, and that subsidiary onward donates those funds for charitable causes, one then has to consider where and when the MLRs apply to those subsidiaries outside the UK. Reg 8(1) of the MLRs impose a geographical constraint on the operation of the MLRs, in particular, the CDD requirements imposed under Part 3 which applies when "acting in the course of business carried on by them in the United Kingdom". We recognise accepting a charitable donation and paying that away to a third-party charity can sometimes be classed as those of a "MSB" for MLR purposes. However, any attempt to apply policies, controls and procedures on a case-by-case basis depending on whether the subsidiary is carrying out activity in the UK is problematic, including relating to MSB activity.

In low-risk scenarios where funds are being transmitted for charitable purposes and remain in the charitable sector, we recommend consideration is given to requirements for Due Diligence measures on the charitable donation. We also believe consideration should be given as to whether the MSBs definitions should apply, including relating to overseas subsidiaries of UK regulated firms.

There needs to be consistency and clarity in determining the scope of the regulatory perimeter, including products/services within specific sectors, rather than ad hoc decisions about overall sectors. For example, social media firms are not within the regulated sector but in September 2021, Twitter announced that it was adding Bitcoin to its Tips feature, which allows users to send money to others through PayPal and other third-party services, and would be rolling that out throughout the world. This would seem an example of activity that should be in scope.

14. What are the key factors that should be considered when amending the scope of the regulated sector?

The key factor is if they bring risk into the system and if so, to what extent, and this assessment should include a focus on both the product and service. We would welcome work to develop a principles-based approach, underpinned by a review of the existing regulatory perimeter by HMG working with regulators, law enforcement and the regulated sector to assess how risk enters and leaves the regulated sector.

This would need to deliver a more granular understanding of risk, particularly when considering ways to strengthen the existing regime, consider what new powers may be needed to stop transactions and allow a more developed base for assessing which sectors should be included. This would be more beneficial than considering on an ad/hoc basis inclusion of a particular sector.

However, it is also important to ensure that, before adding new sectors into the scope of the regime, there is a robust process for determining who will regulate them and that those regulators are adequately resourced/skilled to undertake that role. It would be counterproductive and inappropriate for a lack of effective supervision or management of risks to flow through for the financial sector to manage as is currently the case with for example, MSBs or conducting extra checks on CH data.

15. Are the current powers of enforcement provided by the MLRs sufficient? If not, why?

The MLRs provide a wide range of potential sanctions and enforcements for regulatory breaches. However, application of those powers varies by sector and are not always applied consistently or sufficiently robustly to be adequately dissuasive. Equally, supervisors do not always have the means and resources to effectively monitor and assess risk in their supervised base. For example, the extent of HMRC's supervisory responsibility seems out of step with their resources to perform those functions, especially given many areas they are responsible for are seen in the NRA as higher risk. We refer to OPBAS's latest annual report, which notes that only 26% of PBSs were using their enforcement powers efficiently.

Conversely, the financial sector has faced significant consequences for failures of systems or controls, or non-compliance. This is not only fines but increased regulatory oversight on compliance relative to monitoring, testing and assurance of systems and controls. The regime has resulted in extensive enforcement action to hold firms to account, including significant regulatory fines, criminal investigations and proceedings for criminal breaches of the MLRs, FSMA and other regulation.

It is right that action is taken when there are significant breaches. However, whilst the MLRs and enforcement action has driven more focus and investment by firms, it seems there continues to be failures in common areas amongst firms, despite in many instances, best efforts to adhere to money laundering related obligations. This is regrettable for the firms concerned and for the sector as a whole. It would be helpful to discuss the drivers of this in more detail between the sector, regulators and HMG as the opportunity to better focus resource upon high-risk, whilst reducing low impact activity would potentially bring deliver better outcomes for all.

In looking again at powers, there is an opportunity to seek common risk-based supervision methodologies across all sector supervisors (the new EU-overarching supervisor will issue similar guidance once established) to reduce uneven application of enforcement powers. We also recommend introducing consistency across the current varying approaches towards publicity of supervisory action, as we understand significant proportions of public sector supervisors do not publicise findings.

Equally, whilst the CfE focuses on enforcement, we believe there is a need for a strong focus on prevention and in particular should there be stronger and more effective principles of authorisation of individuals and firms, particularly with regards to a fit and proper person test.

16. Is the current application of enforcement powers proportionate to the breaches they are used against? If not, why?

The FCA has a range of actions it can apply ranging from prosecution to financial penalties to the suspension or cancellation of permission to undertake regulated activity. The evidence suggests these penalties can help change behaviour, as firms have invested heavily into AML/CTF programs, but there is a balance to be struck. It has also created an environment where firms are very sensitive on customer risk, and decisions on whether to enter into business relationships – particularly on-going costs to taking on higher risk customers, or fear of regulatory enforcement if they cannot demonstrate full mitigation of risk with certain customers. Tackling this requires both greater supervisory clarity and other supervisors to raise standards.

We note that the SM&CR is a FCA enforcement tool not available to other supervisors. We recommend rolling out more widely a modified version of the SM&CR regime, underpinned by the right regulatory framework, to other sectors as part of a holistic approach to the promotion of economic crime prevention and corporate good governance. Under this proposal it would apply to all sectors –regulated for AML purposes or not - who have a role in preventing economic crime.

17. Is the current application of enforcement powers sufficiently dissuasive? If not, why?

We believe the current application of enforcement powers is sufficiently dissuasive in the financial sector. However, there is not the transparency of activity in some other sectors, nor does there seem to be sufficient supervisory resources to allow there to be a high chance of sanction. For example, we note that MSBs have been viewed as a high risk for over 15 years now, but the number of actions and prosecutions seems low.

18. Are the relatively low number of criminal prosecutions a challenge to an effective enforcement regime? What would the impact of more prosecutions be? What are the barriers to pursuing criminal prosecutions?

As an industry, banking is subject to the highest regulatory standards; this is to be expected given the size, complexity, and the importance of the sector to the UK. This also reflects that identifying potential vulnerabilities in the financial sector is essential for criminals to launder money. The FCA regularly conducts reviews of the financial sector systems and controls to prevent and detect money laundering and members recognise that this process is more rigorous than in some other supervised sectors.

Therefore, we do not view the low incidence of criminal prosecution under the MLRs as a challenge to the effectiveness of an enforcement regime in the financial sector. This does not necessarily apply to other sectors depending on risk vis a vis supervisory capability.

Further work is needed to understand the impact of the criminal route, which includes the mere threat of such an action being an effective deterrent as receiving a criminal conviction could have significant business and reputational impact on a firm. As a consequence of such an outcome, the firm may not be considered to be 'fit and proper', potentially leading to the loss of licenses or the ability to undertake cross border or payment activity, impacting the firm, and its clients.

In terms of barriers to prosecution, issues such as time to investigate, complexity, information/record availability, and the need to prove to criminal (rather than civil) standards, as well as disproving any defence raised by the defendant, could all be potential barriers.

19. What are the principal barriers to relevant persons in pursuing a risk-based approach?

A true RBA requires and enables firms to focus resource on the highest risks and is central to an effective AML/CTF system. However achieving it requires a legislative, regulatory and supervisory approach, which drives a RBA based on a shared understanding of risk and appropriate mitigation. There are currently barriers in all these areas.
Crucially it also means accepting that some risk will enter the system as a RBA inherently suggests that there will be a certain level of risk existing within the system. However, if this concept is not accepted, and there are severe consequences for any risk existing, it encourages a system that cannot tolerate risk, resulting in unintended consequences such as de-risking.

Legislation and Regulation

We strongly believe the current approach is not working effectively or as intended. Many areas of the MLRs are restrictive and prescriptive, and result in regulatory burdens that tie up resource in low impact activity as opposed to against threats.

Whilst the MLRs seek to balance a RBA with prescribed requirements, they are currently overly weighted towards a prescriptive approach to EDD, even when there is limited money laundering risk, resulting in regulatory burdens contributing to the volume of resource tied up in low impact activity. Examples of these are set out in Annex A.

The complexity of the regime and inflexible, mandatory requirements sufficiently based on risk is a significant challenge. The legislation has shifted away from an RBA with the changes to the 2017 MLRs for example broadly disincentivising the use of SDD resulting in an expensive compliance regime that does not necessarily address underlying problems or risks.

Currently there is little incentive for firms to apply SDD as:

- SDD is optional, with the changes in the 2017 MLRs reducing the practical benefits of SDD,
- the cost to firms of building a defensible risk assessment methodology that permits SDD, combined with the perceived risk of supervisory action and remediation costs if the supervisor disagrees with a firm's application of SDD,
- the cost of building controls to identify and remediate when customers no longer qualify for SDD and the impact on those customers should the firm not be able to complete the additional due diligence,
- supervisory focus typically on higher risk situations and the mandatory application of EDD.

Clearer supervisory expectations on the use of SDD, and what constituted a potentially lower risk situation, would help overcome these challenges.

Another live example is the degree of dissonance between the CDD obligations in the MLRs and the information that can be supplied by vulnerable customers such as those relocated to the UK under the Afghan Relocations Assistance Policy (ARAP). Whilst FCA guidance on vulnerability rightly encourages an understanding and sensitive approach to vulnerable customers, other FCA instructions on Afghanistan or CDD create challenges for firms to manage tensions between regulatory expectations and the needs of vulnerable individuals. We would welcome more clarity on the right RBA in urgent situations such as Afghanistan.

Supervision and Supervisory Expectations

Effective supervision of other sectors is important given the expectations on our sector to carry out EDDon customers already caught within other parts of the regulated sector. Any expectation to conduct EDD and 'know your customer's customer' increases and replicates compliance and limits

adoption of a true RBA as members are expected to act as de facto regulator of other sectors, due to shortcomings in the regulatory approach in those sectors. This encourages a very risk averse approach, and links to the points made elsewhere regarding the need to be able to rely on work, or supervision, being undertaken within the regulated sector.

The strong perception in the financial sector is the current system drives a 'zero failure' approach and that process weaknesses or non-compliance with a procedure can result in supervisory action – irrespective of the total overall effectiveness of a firm's control environment or the risk. The perceived absence of flexibility for minor breaches given to firms who have otherwise invested significant amounts of resource and effort into robust AML controls drives the risk attitude and can mean compliance will be 'gold-plated'.

The need to show compliance means that firms invest significant amounts in auditing and demonstrating that the compliance is rigorous enough and has been checked to the regulator. It means that even where there is limited exposure to true risk, firms will still wish to demonstrate high levels of monitoring to the supervisor to prevent the threat of enforcement action.

This low impact compliance activity comes at a cost and means some accounts become unprofitable to maintain, even in the absence of true risk, as the costs of conducting EDD and monitoring outweighs the commercial benefit and/or where they deem the risk too great to sufficiently mitigate in a way acceptable to the supervisor. This tension seems relatively unique to banking as other supervised sectors appear to have little equivalent problem of 'de-risking' of higher risk customers. Changes set out elsewhere can help address this.

We also believe that uneven supervisory expectations act as a barrier as there are views, as below, that some supervisory staff do not always have the level of understanding of either financial crime, or the risks specific to individual businesses, that would allow them to review their supervised population and promote the application of a risk-based approach.

<u>Understanding of risk</u>

This is exacerbated by the lack of a single public sector view of risk and a fragmented ecosystem. This is why we need system leadership to set a single regime-wide objective that all actors in the ecosystem work towards and are assessed against.

20. What activity or reform could HMG undertake to better facilitate a risk-based approach? Would National Strategic Priorities (discussed above) support this?

It is necessary to address the issues above. National Strategic Priorities, in the absence of changes in legislation, supervisory expectations and the ability to flex resource, would not achieve this. There also needs to be an explicit recognition that no matter the effectiveness of technology, systems, or controls, not every criminal or suspicious activity will be detected, and the financial sector will legitimately take a number of approaches to detect financial crime.

A RBA would be greatly facilitated by the levelling up of financial crime controls and oversight in other sectors and be better facilitated by improved supervisory understanding of the diversity that exists across and within their supervised sectors. Having confidence in supervisory understanding would encourage a more balanced RBA to be followed.

As set out elsewhere, a sufficiently granular single public sector view of risk would also help better facilitate a RBA as would enhanced information and intelligence capabilities that support a better shared understanding of risk, which would in turn promote a more successful RBA.

Ultimately, the reform needed to facilitate needs to deliver a single view of risk supported by a robust information sharing agenda that ensures public and private sector actors are sharing the most valuable intelligence, in as close to real-time amongst the widest possible group of actors. This agenda should extend beyond what is currently planned in the EEC to develop channels in the long term, ideally between private and government data sets, and create an ecosystem of information to specifically assist in the prevention of economic crime.

21. Are there any elements of the MLRs that ought to be prescriptive?

We do not believe there is merit in an overly prescriptive approach but are aware other jurisdictions/territories such as the EU are moving towards that approach. This will either filter down towards UK institutions with EU affiliations, or create dissonance with the EU approach. We believe the UK should promote internationally the benefits of a true RBA.

Increased clarity on acceptable risk mitigation would be a welcome addition, to allow members to mitigate the risks in an agile fashion so we believe there needs to be a mechanism to get a better shared understanding on how to manage risk and to identify areas where further controls are needed. Even then, flexibility is needed, particularly for firms with a diverse customer population operating in many jurisdictions, rather than a “one size fits all” prescribed approach.

Some members would urge more prescriptive requirements on the public sector – namely to ensure they are both providing sufficient guidance to resolve thematic issues such as access to banking challenges, or to show sufficient controls in legislation and regulation to reduce risk.

22. Do relevant persons have an adequate understanding of ML/TF risk to pursue a risk-based approach? If not, why?

We have set out above thematic barriers to a RBA but for relevant persons these can be exacerbated by the lack of a consistent and shared understanding of ML/TF risk. There are many different sources of risk assessment, including different ways to identify and scale inherent risk, control effectiveness and residual risk. We have set out our thoughts on this elsewhere.

Equally this will vary by sector as sectors that have been regulated for a sufficient period and subject to strong supervisory oversight are more likely confident that the risks are managed and understood. However, risks change so additional guidance and support from law enforcement and regulators would reinforce the model in place so there is a need to improve how to disseminate lessons learnt, or typologies discussed at PPOB and JMLIT to all parts of the regulated sector.

In addition, it is important new legislation is considered holistically– so for example, when the MLRs are refreshed, taking the opportunity to consider fraud and boost terrorist financing references to help support relevant person understanding of relevant risks.

We have already commented on sectors that should be included to balance the regulatory oversight of the entire ecosystem and would welcome regulatory and law enforcement education for newer entrants to the market, such as crypto asset/fintech sectors, as well as the established sectors with known gaps. Please refer to our responses throughout for additional detail.

23. What are the primary barriers to understanding of ML/TF risk?

The greatest barrier is that there is no single view of risk stemming from the public sector, and no consistent way to determine inherent risk, control effectiveness and residual risk. As a result, understanding of risk and priorities is inconsistent.

We would also point to overlapping and sometimes contradictory guidance. Many members operate in multiple jurisdictions and in the UK alone need to consider various guidance sources (JMLSG, FCA Financial Guide for Firms, additional FCA guidance/thematic reviews, the UK NRA, HMT and HMRC information etc). This is compounded by international guidance (FATF, Wolfsberg Group), EU and US publications and any other local guidance where we may operate.

24. What are the most effective actions that the government can take to improve understanding of ML/TF risk?

Improvements to the granularity of the NRA would assist given the NRA directly affects supervisory sectoral risk assessments. Whilst the general steer offered by the NRA is welcome, nuances are often missed. For instance, whilst the NRA deems correspondent banking high risk, risks may be lower where a UK-based financial institution with a principally UK customer base wishes to set up a correspondent banking account, or where an EU-based institution wishes to set up a principal-to-principal account (i.e. an account that no customer money flows through).

As above, we believe consolidation of various risk information and intelligence assessments would help improve understanding of ML/TF risk as would broader sharing of information and intelligence from JMLIT. We also believe new powers on information and intelligence sharing to allow greater sharing of information within the private sector are needed, alongside stronger public private activity and two way sharing of risk and actionable intelligence between public and private sector.

Equally, there is a need to reconcile different guidance. There are elements of activity captured in the NRA that may differ from NECC Public Private Threat Assessments – on MSBs for example. A common set of guiding principles in the MLRs for members to apply across all this guidance and/or a "single source" of comprehensive UK guidance would be welcomed.

There is also a need to resolve tensions around understanding of risk that impact access to banking. One example is pawnbroking which is not mentioned directly in the NRA and whilst the National Pawnbroking Association and UK Finance are working to produce shared guidance, this is not the same as officially approved industry guidance. A mechanism should be established for public and private sectors collaboration to address emerging threats, weaknesses in the regime agree risk and risk mitigate and address unintended consequences at pace.

Longer term, the best way of developing such an understanding of ML/TF risk would be tasking a single public sector body – perhaps a system leader - with understanding, coordinating and assessing risk activity across the ecosystem. This seems a role that the NECC would seem suited to play.

25. How do supervisors allow for businesses to demonstrate their risk-based approach and take account of the discretion allowed by the MLRs in this regard?
26. Do you have examples of supervisory authorities not taking account of the discretion allowed to relevant persons in the MLRs?

In answering both questions, members make a number of observations, which also influence the answer below to Q27.

There are many areas where members would point to the FCA as an effective supervisor in terms of their maturity and sophistication in relation to understanding of risk and the full range of the sector they supervise, particularly in comparison to other supervisors of the regulated sector.

Examples that members would point to highlight this, include, the FCA listening to feedback to share their 'Dear CEO' letters more widely. Members find these helpful in terms of understanding FCA concerns and priorities and also note that the FCA MLRO Forum has become a more developed mechanism to discuss issues in a more collective manner.

In the same way, the FCA statement on financial crime during the initial stages of lockdown for Covid-19[4] was welcomed by members as providing the necessary steer and comfort to support members' reprioritisation of activity and ways of working.

The maturity and understanding of the FCA regarding the use and provision of law enforcement intelligence is also strong, as is, for the most part, the separation between FCA involvement in initiatives such as JMLIT – which can require firms to have to demonstrate where they have discovered hitherto unknown risks.

The FCA can also be a powerful force in helping firms more effectively manage thematic risk such as the work with a number of firms on cash-based money laundering.

There is also recognition that there is a great deal of specialist expertise in some parts of the FCA, and the FCA understand the importance and need for economic crime reform; even if the view is, perhaps understandably, that for the FCA to play a greater role in being forward leaning, it requires the legislation and regulations to change.

However, there are also a number of broader observations members have made regarding thematic issues, and individual examples where the approach of the FCA (and other supervisors such as the PSR) have made managing financial crime risk and taking a risk-based approach more challenging; particularly for medium sized and smaller firms where the relationship with their regulators may not be as developed as some of the larger firms.

Conversely there are also examples where it has not been possible to get a clear steer on an issue which in turn either drives a risk adverse approach or means firms have had to decide to operate 'at risk' as opposed to a true risk-based approach.

In setting out the examples below, it should be noted that some members have been reluctant for examples of supervisory engagement to be used, even anonymously. As part of raising standards of supervision across the board, we would urge a mechanism for regular independent feedback on supervisors to support continuous improvement.

In terms of general feedback, there is a view that it has sometimes been difficult to get a 'one FCA' view. There can be different perceptions of the FCA view where understanding from discussions with various FCA policy teams may not then translate into the same stance from supervisory teams. This is broader than just financial crime but is more pressing in this space.

[4] https://www.fca.org.uk/firms/financial-crime/financial-crime-systems-controls-during-coronavirus-situation

Examples would include strategic discussions taking place at senior level about how firms could switch off unproductive TM alerts, when in parallel, following a high-profile case, firms were being repeatedly pressed on why TM systems had not picked this up – even when they explained the false positive rate would have been as high as one positive for every 499 false hits, or even far higher. This kind of exchange can have a dampening effect on risk appetites. It is hoped the recent restructuring in the FCA which will bring relevant financial crime teams under the management of one Executive Director will help ensure a more consistent one FCA voice.

Another general observation is that it is not uncommon for large parts of supervisory teams to be relatively junior and seem to lack the experience or expertise of the relevant business area or financial crime risks of the firm they are supervising. Some members, particularly in smaller and medium sized firms noted that it can appear that supervisory teams often do not have a sophisticated understanding of the risk a firm presents before coming in for supervisory visits.

In setting out these challenges, members also acknowledged the variance in different approaches across the sector and expressed sympathy for the challenges that supervisory teams face in understanding different risk models. Members saw this issue as exacerbated by a lack of time and available documents for supervisory teams to review and consider in advance (which has informed some of the suggestion in Q27 below). However, they did note that this can mean that the level of discussion on risk and approach starts from a low base and could often be repetitive or extended due to the need to reiterate basic risk controls a firm may poses.

This can also create challenges around being able to demonstrate to the FCA why a particular approach is more suitable. A number of members, large and small, have highlighted in particular challenges around getting comfort from discussions with regulators over being able to move towards new technology and systems that are overall significantly more effective if the older systems still pick up some alerts that the newer system may not.

This has led to lengthy periods of parallel running of systems and intensive resource tied up in less efficient systems, even where it can be demonstrated that the new approach allows resource to be focused more effectively towards risk.

A smaller member highlighted how during Covid the FCA guidance seemed to suggest adjustments to TM systems to reduce alerts would be seen as an issue of concern from an FCA perspective, and it was difficult to get a steer if this also included BAU adjustments to a new TM system that had been installed and was delivering excessive false positives.

Other examples from smaller members include where one member had received the Dear CEO Trade Based Finance letter, even though this was not relevant to their business. Another member highlighted how the supervision team acknowledged they were not sighted on what type of business the firm conducted or the type of risks they would handle.

Another member were told by their supervisory team that an MLRO not reviewing all the SARs submitted could potentially be a breach of regulatory requirements – a view that as it had come from a regulator required the firm in question to have to get external legal advice to ensure there was Board level comfort for the approach they were taking.

Given the demand for financial crime expertise, and the flow from the public sector, including regulators, to the private sector there was acknowledgement that it was difficult for regulators to retain and develop the level of expertise they need. It may be helpful, to consider a more

sophisticated model of secondments and open discussions on thematic issues between the regulated sector and regulators.

As well as the engagement with supervisory teams there are other examples where members believe the FCA stance on regulatory interpretation has reduced the ability, at least in the first instance, for firms to take a risk-based approach. These include:

- FCA Guidance on Politically Exposed Persons
- FCA statements on High Risk Third Countries.
- FCA guidance on the listings of cannabis-related business

FCA Guidance on PEPs

Members have some sympathy for the FCA on this issue as there is recognition that this was in part a problem with regards to the 4MLRs that Parliament mandated the FCA to fix. However elements of the FCA guidance can be seen to conflict with elements of the 4MLRs and there was a reluctance by the FCA to engage in detail on this. Aspects of the FCA guidance were also overly restrictive – such as the requirements for all PEPs to require MLRO sign off and again it was difficult to get clarity. Whilst some firms had the confidence to create a framework with MLRO delegation, others, at least initially did not.

However, members do note that whilst this remains a priority to fix, overall FCA guidance was helpful, if compliance heavy, in resolving access to banking issues for domestic PEPs and would point to other access to banking issues that the FCA could help provide clarity on. However, we encourage HMG to review the legal obligation regarding mandatory EDD on domestic PEPs currently in the MLRs that is over and above FATF, as set out in Annex A. Members believe the FCA issuing guidance on this was the right thing to do, given the circumstances. It was the reluctance to engage on the substance of that guidance that caused issues.

FCA Statements on High Risk Third Countries.

Members highlight the dialogue between Trade Associations and the FCA on how changes to the HRTC list - and in particular the addition of Cayman Islands – should be interpreted.

Correspondence regarding EDD on customers residing in new countries added to the UK HRTC list initially highlighted some confusion regarding interpretation of the requirements under Regulation 33(1)(b). The confirmed stance that this requirement does not have retrospective application, i.e., the mandatory EDD only applies to customers at the time the country in which they are established in is listed in Schedule 3ZA, differs from the understood industry interpretation of this obligation.

As per Annex A we believe regulatory amendments are required to address this issue and remove any lack of clarity that exists around regulatory interpretation. However, members did welcome the engagement of the FCA and the eventual clarification, but believe that the clarified FCA position should be formally supported by easily accessible statements. Not all members of the supervised population will be members of the Trade Associations that this view was communicated to, so may not have sight of the expectations here.

We would encourage policy makers and legislators to work with the private sector when drafting new legal obligations in order to clearly articulate the policy objectives, and therefore minimise the risk of over or under compliance.

FCA Listings of cannabis-related businesses

Some members noted that the FCA statement in September 2020 which provided a seeming definitive view that proceeds from recreational cannabis companies, even when they are located in those jurisdictions that have legalised it, are proceeds of crime under POCA, seemed to go further than either external legal advice some firms had received or more pertinently the NCA in response to some DAML SARs firms had submitted.

Some members noted the FCA statement on different licensing requirements in relation to this issue was concerning as there are many areas where business activity can vary in different jurisdictions according to licensing requirements, even if production or sale of those goods in the UK may be a criminal offence. Examples would include firearms or even food standards.

Whilst again, the FCA seeking to provide clarity was helpful, our members would find it helpful if in issuing statements the FCA can set out which different parts of the public sector have been consulted and have approved this position.

27. What more could supervisors do to take a more effective risk-based approach?

There is a need to refine the outputs of the thematic reviews as firms may have different, but effective approaches to AML. Simply highlighting 'good practice' of one area of one bank, means that many others will incorporate an example of good behaviour which may not be needed given the strength of controls elsewhere. This creates a race to 'gold-plate'.

There needs to be a more strategic consideration of the overall effectiveness, and discussion with firms over where they could increase or decrease AML controls within their systems. Sharing what works well and what does not in a system is a subtle but important difference from simply highlighting the FCA view of good and bad practice.

Supervisory staff going in to assess firms should have an improved and consistent understanding of the AML/CTF regime, alongside the nuances between different firms existing within the regulated sector.

Members would welcome more open dialogue with the FCA. This is both collectively and during reviews to be able to set out how their overall approach to AML works, and to have a collaborative discussion over what works well and what does not in the view of the firm and the FCA.

Some members felt that in reviews conducted by some overseas regulators, firms have the opportunity to present and have more open discussions, unlike the UK where it is targeted, and interview based. The relationship needs to be more open notwithstanding there will always be the need for the regulator to take enforcement action where serious failures are identified.

Many members also believe an explicit requirement for the FCA to support effectiveness and efficiency and competitiveness would help support a risk-based approach.

There are sometimes tensions between competing priorities, which can lead members to question where the appropriate balance lies (for example, issues such as access to banking for customers perceived as higher risk and efforts to tackle financial crime). The lack of clear guidance from the FCA on some of these issues can cause ambiguity and leads to extra cost, compliance and can lead to members exiting accounts for commercial reasons.

Members believe that an effective approach would acknowledge requests from members for enhanced FCA guidance in areas that require firms to exercise an element of judgement and of course, in a global banking system, the impact of international regulators on decisions by our members cannot be ignored. However, it will also allow firms in the UK to better justify their approach to international regulators if the FCA has issued clear written guidance.

Members note that an area of benefit could be the introduction of a helpline with the FCA, similar to that available with the ICO. Members could then refer to this helpline when an additional steer is required, particularly with regards to decision making on low impact activity.

28. Would it improve effectiveness and outcomes for the government and / or supervisors to publish a definition of AML/CTF compliance programme effectiveness? What would the key elements of such a definition include? Specifically, should it include the provision of high value intelligence to law enforcement as an explicit goal?

We would cautiously welcome this if it does not expand existing requirements. Members agree key elements would include meeting regulatory requirements, benchmarking with peers, training and education, auditing and monitoring, and effective regulatory oversight and enforcement.

Some members go further and suggest it would be sensible to introduce a more developed AML/CTF effectiveness maturity levels with a set of standardised criteria which will enable rating various components of the financial crime framework (for example “basic”; “developing”; “established”; “comprehensive” and “optimised” covering: 1) policies & procedures; 2) risk assessment, monitoring and acceptance; 3) financial crime staffing; 4) communication, training, and awareness; 5) due diligence and client acceptance; 6) transaction screening; 7) transaction monitoring; 8) ongoing review; 9) quality assurance and MI.

Ultimately, a more effective system-wide approach would define effectiveness with regulated sector contributions flowing from that and be underpinned by regulatory requirements that contain a presumption in favour of a ‘true’ RBA and focus on outcomes. On the latter, this could for example include as part of an approach where Relevant Persons are able to demonstrate:

- that the programme has resulted in detecting relevant high impact activity/customers at the commencement of relationships;
- the programme has resulted in detecting relevant high impact activity/customers during the course of the relationship;
- that appropriate action was undertaken when identified.
- what outcomes their financial crime controls and measures are designed to achieve, and articulate expected changes to outcomes when making changes.

Whilst the provision of high value intelligence is a laudable goal, until there is HMG, regulatory and law enforcement consistency on what even constitutes “high impact” activity, then there will be challenges to achieve the above aspiration. Law enforcement also need to be able to define “high impact intelligence as that is the essential perquisite. We cover this in more depth at Q44 and reiterate our previous comments on the importance of meaningful public/private partnerships.

29. What benefits would a definition of compliance programme effectiveness provide in terms of improved outcomes?

As above, any new definition would need to be principles-based, sufficiently flexible and adaptive to reflect the different environments in which regulated entities operate. If it was used as the baseline for any discussion with supervisors, or to support resource allocation, then it may be useful. However,

if used as another high-level principle or policy statement that is not operationalised, then its impact would be limited.

30. Are the requirements for applying enhanced due diligence appropriate and proportionate? If not, why?

We believe the current EDD requirements are prescriptive and disproportionate. The obligation in the MLRs under Reg 33(3A) is not sufficiently risk-based, as the MLRs mandate the same EDD measures regardless of the assessed risk posed by the customer. In many situations, these EDD measures (including, for example, enhanced ongoing monitoring, establishing Source of Wealth (SoW) of the customer and the customer's beneficial owners, obtaining senior management approval for establishing and continuing the Business Relationship) are disproportionate to the AML/CTF risk posed by the client as identified by the firm. This is promoting a rules-based approach.

While firms are permitted to adjust the intensity of the EDD measures along a spectrum of risk (as per the JMLSG), each EDD measure must still be applied so this clarification (although welcomed by firms) is not sufficient to drive a truly risk-based approach.

Post-Brexit, the UK has aligned its HRTC list to the FATF grey and black lists. However, FATF itself states, under Recommendation 19, that countries on the grey list do not need to be subject to EDD. The EU too is moving towards a slightly more flexible approach in this regard, with EDD still applicable but member states being able to choose from a series of currently entirely mandatory specific EDD measures. Recent discussions amongst member states have also highlighted concerns around the deficiencies of the HRTC regime that the UK has transposed and, is looking towards an approach that is focused on issuing guidelines on trends and typologies of transactions at risk for EU obliged entities, rather than listing third countries. Additionally, because of the requirement to apply the same mandatory EDD measures in each instance, firms cannot tailor their EDD towards the weaknesses identified in the FATF/association organisation mutual evaluations (MER).

This can result in non-value adding activity and harm the competitiveness of UK firms (and their overseas branches and subsidiaries, given that they must apply the same EDD measures) in dealing with these jurisdictions. It can mean firms are not sufficiently empowered to focus their resource on the true threat. For example, while Cayman Islands was recently added to the FATF grey list, the weaknesses identified by the FATF have little relevance when a Cayman fund has a fund manager within an equivalent jurisdiction subject to appropriate AML/CTF regulation/supervision (for example). The practical impact of this, alongside the cost, should not be overlooked; for one member, the addition of Cayman Islands alone would require an additional c.50 FTE.

This is an area where the sector has engaged with regulators to assess the worth of these changes in terms of actually identifying financial crime risk, and to date where it is difficult to see the value added by a mandatory approach over and above how risks have previously been managed. It is an example of where we believe more flexibility with the ability for a targeted approach would be welcome, to focus the additional due diligence on the specific risks.

We believe there needs to be a complete review of the approach to HRTC's more generally, in an effort to realign the UK's approach to one assessing application of EDD measures based on an assessment of the threat posed by each country, one that gives mind to the cost and opportunity costs of implementation across the regulated sector, and supports mitigation of the potential unintended consequences being noted under the current approach. Alignment with the changes being proposed under AMLR, i.e. mandating EDD measures only for black list countries, but allowing flexibility for grey list countries, seems the first step in making these changes.

The current obligation to apply EDD to domestic clients of HRTC generates an administrative burden and takes the first and second lines of defence's focus away from the true high-risk clients. An international firm's high-risk client base across the EU targets firm's resources in a way which may not necessarily be risk-based. This is of particular relevance where a UK firm has a branch or subsidiary residing in one of the high-risk jurisdictions. This may, therefore, be interpreted that all of that branch or subsidiaries' customers are required to be treated as ML/TF high risk on a rules-based approach.

Equally EDD for HRTC is neither a risk based or a nuanced approach, as the risk is based on jurisdiction only – there is no consideration for the entity, product, customer or industry type involved in the transaction or located in the High Risk Third Country. Whilst there is some flexibility in the measures that can be applied, as outlined within JMLSG (particularly under paragraph 5.5.11), recognition of the associated risks would be useful.

As above, we believe the general approach to EDD measures should be risk based rather than prescriptive. EDD should not be triggered unless the customers have been identified as high risk on the basis of a holistic assessment, while considering various factors. For example: a regulated, UK-based Fund Manager with entities incorporated in the Cayman Islands should have its industry and entity type considered, in line with the customer risk factors outlined under Regulation 18 and Regulation 28.

The EDD, alongside wider requirements that need to be considered following changes to the UK's HRTC list can be significant. We strongly believe a grace period should be included following each update to the HRTC list, to ensure firms are given adequate time to consider and update their systems, controls and processes. While the UK has indicated at a high level that it would always seek to transpose FATF lists directly into the UK HRTC list, such pronouncements feature on government webpages and explanatory memoranda to legislation and therefore do not carry the weight of a legal guarantee. This means that firms only gain comfort in the certainty of new HRTC listings when UK SIs are published. This, to date, has occurred twice, with 1-2 working days' notice both times.

There are a number of other areas relating to EDD that we believe require addressing through specific regulatory amendments. These have been set out in more detail under Annex A, and include more detail on:

- EDD mandated measures
- The approach to "complex or unusually large transactions;
- The approach to correspondent trading relationships;
- EDD requirements for PEPs; and
- EDD in HRTCs

The amended MLRs 2019 also introduced changes to Reg 33(6)(b) to note new high-risk factors where "there is a transaction related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory or other items related to protected species, or other items of archaeological, historical, cultural or religious significance or of rare scientific value.") At the time it was noted that the intention of the inclusion here was not understood, and that clarificatory information would be required from HMT. This resulted in the production of JMLSG guidance clarifying considerations to these risk factors under Part 1, Annex 4-II, III Products, Services and Transactions Risk Factors.

We believe that producing lists such as these which set out what should be considered high risk are at odds with the notion of a risk-based approach, particularly when considering that certain risk factors or typologies specifically listed within the MLRs may soon be out of date. It would be more effective if this was linked back into earlier points made around being able to dial up or down activity in line with threat and priorities.

We note further challenges faced by firms include the EDD Requirements for Correspondent Banks, as outlined under Regulation 34 (Enhanced Customer Due Diligence: Credit institutions, Financial Institutions and Correspondent Relationships). The onerous CDD required for Correspondent Banks could be a “high impact” activity, as it’s arguably the largest risk our members face outside MSBs.

All relationships with Credit and Financial Institutions fall within the definition of Correspondent Relationships, Correspondent Banking/Trading relationships. Whilst the Money Laundering Regulations refer to “third country” under s.34(1), for any non-EEA state, there is no nuance to reflect risk associated with the jurisdiction in question.

In order to target the risk effectively, it is our view that there should be a graded approach for jurisdictions representing higher risk – similar to the ‘Higher and Lower Risk PEP’ scenario. Whilst we accept that correspondent banking carries significant risk based on having no direct relationship with the underlying parties to a transaction, the risk would arguably be greater in some jurisdictions as opposed to others – a principle recognised in the HRTC list.

31. Are the measures required for enhanced due diligence appropriate and sufficient to counter higher risk of ML/TF? If not, why?

Whilst the specific measures mandated by the regulations are largely believed to be appropriate, as set out above, we believe there should be flexibility for when these specific measures are applied, in line with the assessed AML/CTF risk posed by the client.

In addition, the lack of nuance under EDD measures can drive what we perceive as low impact activity and prevent firms from focusing resource and attention on the highest risk populations. This runs contrary to providing high quality intelligence to law enforcement.

32. Are the requirements for choosing to apply simplified due diligence appropriate and proportionate? If not, why?

No, we believe the application of SDD requirements is not incentivised and is disproportionate. The allowance as part of SDD for varying the "timing" of CDD measures is unhelpful – by varying the timing, the cost is still ultimately incurred later, and new systems need to be created to detect the deadline for performing such delayed CDD. Reg 37(2)(a) sends a strong overall message that all CDD measures must ultimately be applied.

We are also under an obligation to assess our customer in terms of risk, including products, as per regulations 18 and 28. Regulation 37(5)(a) updated the 2007 position on pooled client accounts, whereby they can be subject to SDD only when deemed low risk. However, this is difficult based on the JMLSG Guidance, (agreed by HMT) which needs to be clarified (for example, further definition of what is meant by the account having a “limited, domestic purpose” under Annex 5-V of JMLSG Part 1) as there is no explanation in the MLRs of what Standard or SDD means practically for PCAs.

Whilst this gap was previously filled by the EBA’s guidelines (EBA/GL/2021/02 section 9.16ff), they are disproportionate, impractical, and have resulted in the access to banking issues we have today. We recognise that JMLSG was restrained by the EBA’s guidelines and therefore had limited options for addressing the challenge. However, Brexit has provided HMT an opportunity to address this challenge by amending the Regs.

33. Are relevant persons able to apply simplified due diligence where appropriate? If not, why? Can you provide examples?

We have set out thoughts on this issue above and at Q19.

Relevant persons are able to apply SDD measures, but due to the overarching obligation to still apply measures as per Regulation 28 and 30A but with the option to adjust the extent, timing or type of measures undertaken, the additional processes and controls associated with undertaking such additional adjustments may often lead to a relevant person deciding to instead undertake 'usual' measures for purposes of efficiency and to reduce regulatory risk. The removal of the list of prescribed products for SDD (2007 MLRs) reduced confidence that firms would not face penalties from the regulator for applying SDD exacerbating this issue.

As above, an example where the unintended consequences of this can be seen is with PCAs. We have set out our concerns on this at Annex A, and shown how these concerns have resulted in the common scenario seen today, where the stringency of the requirements result in the product becoming commercially unviable, and challenges around access to banking.

It also links into conversations around supervisory effectiveness. We view the extent of current obligations applied by financial institutions to regulated customers' PCAs as an indictment of supervisory effectiveness – members should not be asked to perform the role of a secondary supervisor but should instead trust that someone who remains a regulated sector firm is in fact compliant with the MLRs – or else they would surely face regulatory repercussions.
Ultimately, if firms have to continue to in effect treat persons whose funds are held in the accounts as beneficial owners (in terms of the CDD obligations applicable to such persons), when in fact the percentage of funds in a PCA that might be owned by such persons could be negligible and significantly below either the Regulation 5 percentage thresholds or "control" criteria, then the products will be withdrawn/restricted from the market because it is operationally impossible (and both ineffective and inefficient) to do so.

34. Are requirements for choosing to utilise reliance appropriate and proportionate? If not, why?

No, we believe there is little incentive to be relied upon, when considering the need for the firm being relied upon to build a control framework and an audit programme to assist the relying firm to comply with their obligations under Reg 39. An example is where the party being relied upon will delete the records five years after the mutual customer ends their relationship with them, but under Reg 39.1, it is the party that is relying on the records that holds the risk if this happens, not the other way around.

Whilst we are conscious that this change stems from FATF wording "without delay" in particular, the wording used is disproportionate; a requirement for "immediate" provision of documents or information puts great demand on firms and therefore becomes disproportionate.

35. Are relevant persons able to utilise reliance where appropriate? If not, what are the principal barriers and what sort of activities or arrangements is this preventing? Can you provide examples?

Members believe that the concept of 'reliance' is not as helpful as previously, as firms still have to obtain information, screen and ingest this into systems. As above, we are conscious that this change stems from FATF wording to "immediately obtain necessary information." However, without further clarity the potential of Digital ID will be fettered by each firm needing to replicate checks carried out by others.

Our members note this balance has been achieved successfully elsewhere in a way compliant with FATF requirements, such as the approach taken in Canada which provides the ability for banks to rely upon other local banks and Government Agencies (captured under section 5 of the act) who

have already verified the identity of a customer. This has been welcomed by members with a presence in Canada and we have included the relevant legislation under Annex C.

36. Are there any changes to the MLRs which could mitigate de-risking behaviours?

There are a number of ways to achieve this which we have highlighted above.

The main way to mitigate challenges to banking issues is recognition that so called de-risking behaviours are the consequence, albeit an unintended one, of a regime where it is relatively easy for the cost of compliance to exceed the value of banking that customer, and where business risk appetites will also be driven by concern over the stance of the regulator.

To tackle this needs the adoption of a RBA as set out in the examples shown above. This would stem from clearer interpretation of existing AML rules across existing sources, alongside regulatory acceptance that risk-based controls can be flexed in line with a business and customer's assessed ML/TF risk.

The second is to actively change the legal and regulatory framework to reduce the cost of compliance through measures that add excessive cost but do not support active management of risk, such as some of the changes on PCAs or on EDD listed above.

The final way is to reduce the fear of regulatory action through improved and targeted guidance from supervisors on thematic issues, such as appropriate controls for pawnbroking, and making clear that, in line with the above, if these were in place and there were no other warning signs, then this would be sufficient to support a RBA even if some minor money laundering risk later emerged to have materialised.

Refocusing resource on high impact activities under a true RBA will help to address access to banking issues. However, where a firm does not believe that it can effectively manage the financial crime risks associated with a business relationship, it should not enter into or maintain that business relationship. This is in line with legal obligations and international standards and it is therefore the correct outcome for individual customers to be exited or declined for this reason.

37. As currently drafted, do you believe that the MLRs in any way inhibit the adoption of new technologies to tackle economic crime? If yes, what regulations do you think need amending and in what way?

The MLRs are technology neutral and do not actively discourage the use of new technologies. This should remain so it is rather the role of regulatory and industry guidance to provide instructions on, and encourage the use of new technologies, where these can contribute to tackling financial crime.

The current regulatory stance does not go far enough with regards to encouraging the uptake of new technologies. There is a lack of confidence with regards to regulatory acceptance when it comes to the use of new technologies which needs to be addressed. Again, a requirement for supervisors to take a more activist role in supporting effectiveness and efficiency and providing guidance on thematic issues would help.
Further guidance is needed to clarify application of certain technologies including for example, how to assess the level of assurance when leveraging Digital ID, or the use of AI in terms of definition and further usage. In addition, guidance from the FCA regarding expectations for new technologies, e.g. expectations regarding calibration and testing, could also help to provide comfort.

In a practical sense, one blocker is, particularly amongst larger institutions, the need to calibrate and integrate these technologies across a number of existing legacy systems. This links to the points above around low impact activity and effectiveness. Regulatory comfort on what standards have to be met to be able to turn off legacy systems that are providing little AML/CTF impact, and updating them with more efficient technology, would help encourage the uptake of new technologies.

In terms of more specific challenges, members have set out the below:

Digital Identity

It will be important to understand how regulatory requirements will be met. For example, Reg39 covers outsourcing of CDD measures, whereby a relevant person can rely on a third party to apply them, but it would be useful to understand if HMG foresee a specific regulatory reference to firms relying on a central repository of CDD data, or whether this would be reflected solely in JMLSG. We set out our thoughts in Annex C on the Canadian model, an approach we believe could work.

We note the members believe there is great potential for Digital ID to transform the approach on KYC if the right regulatory comfort can be provided.

Privacy Enhancing Technologies (PETs)

Use of biometrics to support cybersecurity and storage of customer data continues to develop. Whilst the existing regulations can be interpreted to support use of these technologies (for example, Reg 28 and 33 are not prescriptive on how we obtain additional information on the customer or beneficial owner). Specific reference to this in the legislation and supporting guidance would be useful to ensure the right balance is struck. Whilst JMLSG does refer to the use of biometric data[5], it is broadly absent from the NRA. Specific guidance would preclude the need to obtain regulatory approvals for the use of these technologies.

Open Banking

We have provided our views on AISPs, PISPs and Crypto assets under the Statutory Instrument Response, and would make the same points here.

38. Do you think the MLRs adequately make provision for the safe and effective use of digital identity technology? If not, what regulations need amending and in what way?

We have set out elsewhere potential barriers to use of Digital ID and how to address them.
We would further note there are tensions between the requirements set out in the MLRs, and those that exist in Digital ID guidance, such as the Good Practice Guide (GPG).

39. More broadly, and potentially beyond the MLRs, what action do you believe the government and industry should each be taking to widen the adoption of new technologies to tackle economic crime?

We should strive towards achieving a principle based, technology neutral set of regulations and guidance, which are understood by all parties within the regulated sector, which are suitably adaptable for rapidly changing technological environments.

[5] Part 1, under section 5,

As outlined, this also needs proactive support from regulators and supervisors who should have an explicit focus on effectiveness and efficiency and competition.

40. Do you think the MLRs support efficient engagement by the regulated sector in the SARs regime, and effective reporting to law enforcement authorities? If no, why?

In theory yes, limited only by the capacity and capability of supervisors to ensure this is happening, and the level of law enforcement resource to engage. However, there are gaps in capability and capacity across all supervisors and insufficient resources in law enforcement.

There is a lack of understanding and feedback on thematic risks and issues arising from SARs on a sectoral basis, let alone to allow comparison of peers within a sector. A welcome aim of the SARs Reform Programme is better feedback from law enforcement around SARs reporting, what constitutes a good SAR, and what constitutes high value intelligence. If the role were to be enhanced to consider the quality of SARs within the supervisors regime, perhaps any powers afforded to the supervisor should be more around education to the firm, to rectify and ensure that better quality SARs are submitted in the future.

This also needs legislative and regulatory flexibility to dial up, dial down or stop reporting (or discharge reporting obligations in a different way to prevent the use of SARs to supplement S7 reports to the NCA) and a system leader with the power to provide direction.

Given the volume of SARs that are submitted each year, firms are already under considerable pressure and there are already extensive legal/regulatory obligations around SAR reporting. To the extent that it is determined that a SAR has not been raised when it should have been, there are already serious consequences as a result of this under POCA and the MLRs

Members believe that legislation would be more effective and the CfE is not explicit enough regarding the links to POCA and wider reform. NCA engagement has provided a growing overview of unnecessary reporting required by law so there needs to be the ability to stop or reduce unnecessary or low impact reporting driven by POCA requirements and in turn to de-prioritise or stop the activity under the MLRs that leads to those reports.

41. What impact would there be from enhancing the role of supervisors to bring the consideration of SARs and assessment of their quality within the supervisor regime?

There needs to be consideration given to the capacity and capabilities of individual supervisors, if their responsibilities are increased in this way, as we struggle to see how this would work. It is for law enforcement to decide if a SAR is of good quality, and equally many SARs may not demonstrate their value until several years after the event. This could drive further tick box reporting as opposed to high value intelligence.

Whilst we appreciate there may be benefits in supervisors having access to SAR information, this is limited when considering SARs on an individual basis. Without the ability to see wider submissions to the NCA, there will be limited benefit in viewing on a SAR-by-SAR basis.

Ultimately the authority best placed to evaluate the quality of SARs and their value is the NCA and as such it is for the NECC to assess the overall quality of reporting by sector and to address sectoral

and individual firm failings as necessary through feedback and if needed engagement with the relevant supervisors.

We are aware of significant ongoing work under the auspices of the ECP to ensure that UK FIU are able to provide more feedback to reporters specifically on the issue of the quality and impact of SARs. Providing supervisory authorities with access to SAR information and tasking them with also evaluating their quality could lead to a disjointed and duplicative approach which may not lead to effective supervision, and drive up low impact activity.

42. If you have concerns about enhancing this role, what limitations and mitigations should be put in place?

As the quality of SARs can be seen as an integral part of an effective AML/CTF programme overall, it may be more efficient for the NCA to share aggregated information on the usefulness/quality of SARs per firm with the FCA in order to give the FCA an overall view of the firm's SAR filings. This could include, for example, the number of SARs considered useful to LEAs, number of SARs with quality issues etc. but without sharing the content of these SARs with the FCA for quality assessment.

The FIU, or the NCA could also produce periodic reports indicating strategic impact or risk indicators based on SARs filed over time, considering Strategic National Priorities. These could then be shared with supervisors and regulated entities. Using the available intelligence in this way would help enable obliged entities to incorporate identified priorities or risk indicators into their AML programme. In addition, supervisors could also prioritise their areas of supervisory focus based on these reports, and further develop their understanding of how these priorities could be reflected within their supervised population's compliance programmes.

There are lessons to be learned from FinCen and AUSTRAC, who demonstrate the impact of strategic intelligence and risk indicator projects, in terms of SARs filed over time, aligned to clearly articulated priorities subsequently passed on to obliged entities.

In terms of supervisory access, as above, there are concerns regarding the usefulness of supervisors having access to single SARs, as often these become more valuable when considered as part of a much wider analysis.

There are also concerns regarding data storage and safety. It is not understood how all supervisors would intend to store the information received, and whether this would be able to be stored safely within existing capabilities. This is pertinent to the use of powers to share suspicion across the regulated sector. There are also concerns regarding whether different supervisors would be able to manage this additional responsibility within existing capabilities.

If HMG wish to purse this, supervisors should have established and transparent criteria in place which set out how SARs should be used once received, which would then help to frame exactly when and why SARs are requested.

Equally to avoid tick box reporting – as the FCA can fine firms when the NCA cannot – it should be explicit that the content and either reporting or non-reporting of a SAR(s) should not be the basis for enforcement action. The MLRs and POCA should align, but firms should be able to assess suspicion in relation to reporting without fear or favour of regulator action.

43. What else could be done to improve the quality of SARs submitted by reporters?

Many of the themes set out below are also explored in our SI response. Improving SAR quality and reporting standards across the regulated sector needs to involve regular feedback from law enforcement. Direct feedback from the NCA to sectors and firms is the most effective way to enhance the quality of SARs especially where intelligence was not useful, and why.
As part of this, greater clarity should be provided for firms on where and how SARs supported law enforcement activity and the outcomes. This feedback would enable firms to enhance their controls, by, for example, targeting specific client groups and improve SAR filings.

Some members believe that if the NCA could provide more individual and aggregated feedback to firms and sectors on the quality of their SARs in terms of content and usefulness this would improve the quality of reporting and significantly reduce defensive reporting.
Equally, the NCA publishes guidance on better quality SARs, and this could be supplemented by regular updates to that guidance with examples of "poor quality" behaviours.

Outside of these suggestions we would repeat our call for a system leader to have the powers to dial up, dial down and switch off or switch on activity in relation to SARs reporting. This links to the need for wider SARs reform, including legislative change, to radically reduce the volume of low value reports.

44. Should the provision of high value intelligence to law enforcement be made an explicit objective of the regulatory regime and a requirement on firms that they are supervised against? If so, how might this be done in practice?

In principle, the provision of high value intelligence to law enforcement is a helpful aim for the system, but in the absence of clear metrics, there are questions around what high value intelligence would look like, and how firms would be held to account towards these objectives. A key measure of success for each firm would involve feedback from the NCA at the firm level on quality and usefulness of intelligence provided. That seems unrealistic.

Currently there is no test for high value intelligence, as we can only test against, for example, the reporting requirements set by the NCA. Provision of high value intelligence would need both greater clarity from law enforcement on what intelligence they wanted, and the ability for firms to deprioritise other low impact activity without fear of supervisory.

The criteria by which supervisors would assess the quality and usefulness of a SAR are unclear, and it is not clear whether and how these would differ to the criteria contained in existing NCA guidance. If existing NCA criteria are to be used, then the NCA in our view remain the agency best placed to assess the quality and impact of SARs and provide feedback to reporters.
Finally, this reinforces our view on links between MLRs and POCA – and also the need for POCA reforms. There are some SARs that members do not want to file and the NCA do not want to receive, but there is no 'safety valve' in POCA to switch off reporting.
If this were to be implemented, the industry would welcome a workstream on this with the public sector, to ensure that it is proportionate.

45. In your view does the current guidance regime support relevant persons in meeting their obligations under the MLRs? If not, why?

The current guidance regime does broadly support relevant persons in meeting their obligations under the MLRs.

However, this could be strengthened by considering the areas of inconsistency that exist within existing guidance, e.g. tensions between FCA guidance on PEPs. These are set out in more detail in Annex A.

There are mixed views across members regarding the merits of whether there should be a single source of guidance for the entire AML/CTF regulated sector, although members do acknowledge the challenges this would pose in reflecting and addressing sector specific nuances.

46. Is it effective to have both Regulation 26 and Regulation 58 in place to support supervisors in their gatekeeper function, or would a single test support more effective gatekeeping?

It is our view that Reg 26 (Prohibitions and Approvals) and 58 (The 'fit and proper' test) are sufficient, when viewed in conjunction with SMCR requirements and the FCA SYSC rules provisions.

47. Are the current requirements for information an effective basis from which to draw gatekeeper judgment, or should different or additional requirements, for all or some sectors, be considered?

By definition it cannot be, as the NRA repeatedly highlights certain supervised sectors as high risk, and that is often partly due to the inability for supervisors to address those risks once in the system. We believe the current approach to gatekeeping is not sufficient, and is resulting in inconsistent and uneven approaches across the regulated sector. As a result, certain sectors such as the financial sector have to act as de factor gatekeepers to the system. Enhanced gatekeeping measures should remain in place for higher risk sectors such as cryptoassets.

48. Do the current obligations and powers, for supervisors, and the current set of penalties for non-compliance support an effective gatekeeping system? If no, why?

We would repeat the points above. By definition, and by repeated law enforcement assessments, some sectors, and firms within those sectors, pose an excessively disproportionate risk compared to the size of their firm and activity. Nor can our members simply rely on the fact that other parts of the regulated sector are supervised and have been allowed through the 'gate' to bank them.

49. To what extent should supervisors effectively monitor their supervised populations on an on-going basis for meeting the requirements for continued participation in the profession? Is an additional requirement needed for when new individuals take up relevant positions in firms that are already registered?

Any introduction of new supervisory requirements and monitoring needs to be carefully considered – we would recommend a risk-based approach to this, based on the NRA risk ratings of each sector under consideration, and a consistent, transparent set of criteria.

Where any newer industries are brought into scope, they should be subject to heightened monitoring, similar to the cryptoasset regime under Reg 74.

50. What barriers are there to guidance being an effective tool for relevant persons?

The current guidance helps but does not fully support relevant persons in meeting their obligations under the MLRs for the reasons we have set out above. This includes both where guidance exists

but the MLRs are overly prescriptive, or where it is not possible to get a sufficient steer through guidance from supervisors to give comfort on a thematic issue.

One way to strengthen guidance is to resolve areas of inconsistency that exist– such as FCA guidance on PEPs – and to align different pieces of guidance.

For example, members view the JMLSG and the FCA's Financial Crime Guide as written from different perspectives and taking different approaches with respect to AML guidance.

The JMLSG is a more holistic overview of the legal and regulatory framework for AML/CTF requirements and interprets the requirements of the relevant law and regulations, and how they may be implemented in practice. It provides an indication of good industry practice in AML/CTF procedures through a proportionate, and RBA to assist firms to design and implement the systems and controls necessary to mitigate the risks of money laundering and the financing of terrorism. The FCA's Financial Crime provides more practical information for firms on actions they can take to counter the risk of financial crime and is primarily drawn from FCA thematic reviews where they observed the good and bad practices of firms they have inspected.

For members, whilst both products serve different needs, they do at times provide different steers to the right approach, particularly given the points on FCA reviews as above. Domestic PEPs are a good example of this tension, as set out in Annex A. Members believe discontinuing either completely is not desirable- they serve different purposes, both of which are helpful. Merging the JLMSG and the Financial Crime guide into a new product is one possible approach. As set out above there is also a need for greater guidance from the FCA on 'touchstone' issues.

There are mixed views across members regarding the merits of whether there should be a single source of guidance for the entire AML/CTF regulated sector, although members do acknowledge the challenges this would pose in reflecting and addressing sector specific nuances.

51. What alternatives or ideas would you suggest to improve the guidance drafting and approval processes?

In addition to the above, members have noted the following points:

- Consolidation of the number of instruments that need to be considered to understand legal obligations would help to remove some of the challenges;
- Reviewing areas of inconsistency between existing guidance would be beneficial;
- A mechanism to specifically request regulator guidance on thematic issues is necessary;
- Clearly marking up changes in previous regulator guidance would be helpful – the recent update to the FCA's Financial Crime guidance which primarily changed dates, which was not made clear, is an example here.

We suggest the industry liaises with the regulatory bodies and law enforcement to share internal intelligence via a bespoke public-private partnership exercise for any "single source" guidance/rulebook or revised NRA process. This could support intelligence gaps noted in the NRA, where firms have identified risks that may not necessarily be reported under the SAR process. It may provide a benefit for smaller firms with a less diverse customer population. The industry would need to be directly involved in the drafting process and be able to provide meaningful input/insights to any proposed changes.

52. What are the strengths and weaknesses of the UK supervisory regime, in particular those offered by the structure of statutory and professional body supervisors?

We believe the biggest weakness is inconsistent standards and approaches across the UK's current supervisory regime. There needs to be a consistent approach to reviews introduced, potentially supported by a common cross-sector supervisory methodology, which would in turn encourage more consistent expectations around standards.

Another significant weakness is the failure to consider at drafting stages of the MLRs whether bringing new sectors within scope of the MLRs would be adequately matched by supervisory capabilities. The FCA for instance have demonstrated some concern in relation to their ability to effectively supervise cryptoasset businesses. While the open admission of the challenges is welcome, FCA capability and resourcing should have been considered and adequately enhanced before bringing additional sectors into the regulatory fold.
There needs to be a levelling up of standards across the supervisory regime, ensuring all supervisors are resourced and capable of performing to the same standards. It is clear that some supervisors, such as HMRC, due to the make up of their supervisory population and their existing capabilities, are not adequately resourced to be able to fully address the risks in their supervisory sector.

The consequence of this fractured supervisory regime is that it allows risks that should have been prevented from entering the system. We set out above how this impacts our members and customers and also contributes significantly towards spending resource towards low impact, duplicative activity.

We believe we should be exploring a "polluter pays" principle, where those bringing risk into the system are faced with equivalent supervisory consequence, rather than it being the expectation that others within the system make up these shortfalls.
An option could be to explore whether OPBAS would be the body that could set standards for supervisors, or even provide the resource to undertake supervisory visits, in an effort to encourage consistency. This is explored in more detail in later questions.

Another weakness is that we have noticed a mismatch between supervisors policy intentions, and the messaging coming out from their supervisory visits which we have addressed above.

53. Are there any sectors or business areas which are subject to lower standards of supervision for equivalent risk?

The FCA is recognised as overall an effective regulator in terms of issuing fines and enforcement actions, and in continuing to strengthen their risk-based supervision. However, we believe certain sectors are subject to lower standards of supervision for equivalent, or even higher risks. As above, this is partly due to limitations in capacity and capability of other supervisors.

Equally, the current 'diffuse' regulatory structure is fragmented, with responsibilities split across the Home Office and HMT. There are 25 bodies that supervise the UK's compliance with the Money Laundering Regulations. The UK NRA identified issues in relation to the Financial Conduct Authority (FCA), HM Revenue & Customs (HMRC) and professional body supervisors' risk-based approach to AML/CTF supervision. Whilst these are being addressed, it does increase vulnerability.

A well-known example is MSBs which is a long standing and recognised vulnerability to which law enforcement has repeatedly drawn attention via threat assessments and public statements, but where the approach on supervision, driven by a lack of sufficient resources, has not seemed consummate to the risk, with instead an expectation the financial sector will monitor risk.

Equally for example, enhancement of HMRC's supervision of the sectors it is responsible for is part of the ECP. We understand that HMRC supervises a diverse range of high-risk sectors and it is developing a more comprehensive and robust risk-based strategy. Planned compliance interventions with businesses not meeting the standards was due by 2021, however the impact of Covid has extended this to 2022.

Whilst this progress is welcomed, limited fines and enforcements calls their effectiveness into question. MSBs pose a large risk to the banking industry and robust supervision is essential. Some members support that supervisory responsibility for this sector moves to the FCA, as concerns exist around resourcing levels in HMRC to manage the risk.

Another area we would highlight is the Pension Regulator. Following high profile pension insolvencies (BHS & Carillion), it is hoped that the new Pension Schemes Act 2021 will strengthen the powers of the Pension Regulator following the Carillion collapse.

However, this Act will take time to embed. We are aware that pensions can be viewed as a lower risk sector, however their susceptibility to financial crime should not be underestimated, primarily due to volume of transactions and investment of the funds in question so the Pension Regulator will need sufficient focus and resources on financial crime.

54. Which of the models highlighted, including maintaining the status quo, should the UK consider or discount?

Some members welcome the proposed degree of consolidation of the supervisory regime, towards the suggested model with fewer, very few, or even a single supervisor. Whilst it is noted that even if there was a “single supervisor”, there may still be fragmentation within the structure, based on areas of expertise, the current approach that makes up OPBAS is sub-optimal so a middle ground is needed.

It is less about any particular model than the best way of delivering a consistently effective approach to supervision underpinned by sufficient powers, resources and a common set of principles and objectives to ensure the ecosystem is a resistant to financial crime as it can be. At the moment, the current approach is uneven, exacerbated by inconsistencies and fragmentation of approach.

Any shift towards a new approach needs to be carefully managed to address known capability and resource issues, as otherwise disruption of the current model could result in more, not less fragmentation in the system. Equally, we note that many of the high-risk areas could benefit from increased resources and investment in bodies such as HMRC, accompanied by a strengthening of the controls and requirements for firms to become approved and a stronger fit-and-proper-person-test and licence to operate.

55. What in your view would be the arguments for and against the consolidation of supervision into fewer supervisor bodies? What factors should be considered in analysing the optimum number of bodies?

The main argument for the consolidation of supervision would be around removing existing inconsistencies, and the generation of a more coherent supervisory picture. As above, this could help to promote a more effective AML/CTF system, as there would be confidence that all members of the regulated population were being held to the same standard.

However, consideration would need to be given to which supervisors, if any, have the capabilities to be able to support the breadth of supervised population that would exist if combined. In addition, understanding of the breadth of different businesses that make up these supervised populations would be even more diverse, so appropriate training would need to be considered for any expanded supervisory body. Alternatively, it may be that there are one or two bodies, within which exist separate divisions covering each of the supervised populations. The benefit is that the desired expertise is retained and focused but there is the benefit of those separate components leveraging governance, resource and expertise from the wide body. We set out alternatives below.

56. What are the key factors that should be considered in assessing the extent to which OPBAS has met its objective of ensuring consistently high standards of AML supervision by the PBSs?

It is not always clear what success criteria OPBAS are working to. It would be beneficial for these to be more widely known and evidenced that these are being measured against.

57. What are the key factors that should be considered in assessing the extent to which OPBAS has met its objective of facilitating collaboration and information and intelligence sharing?

Some members note that OPBAS has made progress in terms of collaboration with law enforcement and the NECC via Intelligence Sharing Expertise Working Groups. However, professional enablers are still identified as a key risk for money laundering/terrorist financing, experiencing limited fines, calling into question the effectiveness of OPBAS' supervision.

In addition, whilst the ECP's Statement of Progress highlighted progress in terms of efforts to increase the consistency of their supervision, it noted that some professional body supervisors have not progressed at the pace required. We understand that they are testing the effectiveness of the AML supervision of the various bodies and will complete this in 2021.
In the absence of more transparency of activity, it is difficult for us to assess that OPBAS can fully demonstrate consistency across the 22 bodies in question, which would be the key factor for assessing the extent to which OPBAS has met its objective of ensuring consistently high standards of AML supervision by the PBSs.

58. What if any further powers would assist OPBAS in meeting its objectives?

We believe the existing regime should be improved or strengthened by giving OPBAS the authority to properly supervise and hold to account the supervisors they oversee as one way of levelling up standards. This would include the ability to raise 'gatekeeping tests' and to strengthen 'fit and proper' person tests. It would also require OPBAS to be able to direct more information gathering from supervised populations and to direct more targeted enforcement.

We also think OPBAS could play a greater role in introducing more consistent standards across supervisors. This could take shape in the form of the production of a rulebook, that the entire regulated sector could be held towards. In addition, we believe OPBAS should be responsible for the creation of a methodology for external AML/CFT supervisory audits and for the training and/or accreditation of the persons undertaking those supervisory audits. This would ensure consistency of standards, alongside a way to assess supervisory standards.

59. Would extending OPBAS's remit to include driving consistency across the boundary between PBSs and statutory supervisors (in addition to between PBSs) be proportionate or beneficial to the supervisory regime?

In theory we think it would, aligned to a common set of principles and objectives across the regime and the resources and powers to drive that. However, whilst we welcome the introduction of the sectoral intelligence sharing expert working groups (ISEWGs) led by OPBAS, there is limited output and visibility outside the UK NRA. We suggest as an interim step, the financial sector industry and UK Finance should be involved in this intelligence sharing to promote effective public-private partnerships, as it seems currently limited to other regulatory bodies and law enforcement.
Whilst OPBAS' input into the NRA is welcome, and resulted in focused NRA sections on the accountancy and legal sector, the industry would benefit from further dissemination of intelligence linked to this sector. This would allow us to collectively develop our RBA to this sector.

60. Are you aware of specific types of businesses who may offer regulated services under the MLRs that do not have a designated supervisor?

We are not aware of businesses offering regulated services under the MLRs that do not have a designated supervisor. However, there is a bigger challenge around unregulated entities that at face value advertise or provide services as business activities that would seem to fall within the MLRs or where there is a lack of clarity. Examples include:

<u>Tax Advisor</u>
Since 10 January 2020, the definition of a tax adviser under the MLRs 2017 has changed and become wider in scope to be: 'a firm or sole practitioner who by way of business provides material aid, or assistance or advice, in connection with the tax affairs of other persons, whether provided directly or through a third party, when providing such services.'

This is very broad and could be read as including incidental services (for example, the provision of software that helps customers determine their tax liability). In particular, we would note it includes "assistance...in connection with tax affairs of other persons whether provided directly or through a third party". Clarity would be welcomed so all are aware of their responsibilities, and excluded activities are made explicit.

<u>Unregulated Accountancy Services</u>
Some members note that multiple accountancy firms remain unsupervised due to the number of accountancy sector supervisors, and HMRC as a last resort, creating too many opportunities for firms to slip through the net and remain unregulated.

We note that anyone can call themselves an accountant, there is no need to have any qualifications; have undertaken any Continuing Professional Development (CPD); demonstrated any relevant knowledge or to be a member of a recognised professional body. According to HMRC in 2019, approximately two thirds of complaints they receive about agents relate to unregulated practitioners. We agree with accountancy sector bodies that any unregulated agents should be brought into scope of the MLRs and be subject to both OPBAS' oversight and complaints and disciplinary processes.

<u>Unregulated Legal Services</u>
Individuals who have been struck off can continue to provide legal advice and not all legal activities are regulated. For example, the FCA only regulates lawyers who provide investment advice. Areas not regulated for MLRs includes will writing and estate administration, family, and intellectual property law – so many practitioners can offer a variety of services, not all of which are regulated, and it is often difficult for a financial sector firm to assess any underlying risks.

There is a conflict in the HMG perception of the risk of unregulated legal services, with the PCA approach treating firms offering such services as particularly high risk, even though such services have been recognised as sufficiently low risk to escape being regulated under the MLRs.

"Lawtech" is another emerging sector (for example, software providers). For firms providing financial services to these customers, clarity would be welcomed so we can adjust our RBA accordingly.

61. Would the legal sector benefit from a 'default supervisor', in the same way HMRC acts as the default supervisor for the accountancy sector?

Some members agree and point to the 2020 University College London report in association with the Legal Standards Board UK which reviewed the UK regulatory model for the legal system in the UK, and concluded that the regulatory framework for lawyers needs better to reflect "the legitimate needs and expectations of the more than 90% of the population for whom it is not currently designed". It called for amongst other things, a single, sector-wide regulator of all legal providers and a single point of entry for consumer complaints.

Many of those members highlighted the 2021 report by the Law Society[6] which identified that key non-compliance trends in Legal Service Providers (LSPs) observed by PSBs included many LSPs treating AML compliance as a low priority or a tick box exercise which comes second to their day job. In addition, they identified insufficient or weak risk-based controls and a lack of legal sector specific AML training available for LSPs. There is a view that the low compliance of a significant amount of LSPs has enabled criminals to exploit the sector considerably and therefore, a default supervisor would be welcomed.

Others do not have strong views on this question, but note that the supervisory model for the legal sector, with one dominant supervisor (Law Society) and regulatory authority (SRA), means there is less room for legal sector firms to remain unregulated.

However, other members point to the effectiveness of that supervision, and note they will engage with transactions on large value properties where there are other underlying risk factors, and as such file a SAR and/or change a client relationship, but there is no evidence the law firm has done so.

62. How should the government best ensure businesses cannot conduct regulated activity without supervision?

Whilst this consultation has given us a valuable opportunity to provide feedback and areas for consideration, we also recognise that it has identified significant gaps or areas for uplift.

We believe increased public/private partnership is the most suitable mechanism to support HMG in preventing unsupervised regulated activities and to allow law enforcement, government agencies and the regulated sector to work together to drive swift, decisive change where needed.

[6] https://www.lawsociety.org.uk/en/topics/anti-money-laundering/uks-third-national-risk-assessment-published

ANNEX A

Areas of consideration for regulatory change

There are a number of areas within the existing regulations where we believe the current drafting, or lack of clarity regarding the current drafting, is promoting disproportionate application of obligations across industry.

Considering the focus on ensuring the removal of low value or prescriptive activity from the UK's AML regime, we encourage introducing the amends below to realign obligations towards a more proportionate application of intended AML/CTF measures.

1. Enhanced Due Diligence

a. EDD mandated measures

The existing obligation in the MLRs under Reg 33(3A) is not sufficiently risk-based, in that the MLRs mandate the same EDD measures regardless of the assessed risk posed by the customer. In many situations, these EDD measures (including, for example, enhanced ongoing monitoring; establishing Source of Wealth of the customer and the customer's beneficial owners; obtaining senior management approval for establishing and continuing the Business Relationship) are disproportionate to the AML/CTF risk posed by the client as identified by the firm.

This is promoting a rules-based approach. Although firms are permitted to adjust the intensity of the EDD measures along a spectrum of risk (as per the JMLSG), each EDD measure must still be applied. As such, this clarification in the JMLSG (although welcomed by firms) is not sufficient to drive a truly risk-based approach, resulting in inefficiencies across the sector.

This links to the points made in our Call for Evidence response, highlighting the FATF Recommendation 19 messaging calling for countermeasures against black-listed countries, contradicting with the UK's approach, reflecting and requiring EDD on both the grey and black-lists. The practical impact of this should not be overlooked; for one bank, the addition of Cayman Islands alone would require an additional c.50 FTE. Recent discussions amongst member states have also highlighted concerns around the deficiencies of the HRTC regime that the UK has transposed, and is looking towards an approach that is focused on issuing guidelines on trends and typologies of transactions at risk for EU obliged entities, rather than listing third countries. As a result, there needs to be a review of the approach to HRTCs more generally, and the implementation of an approach allowing EDD measures based on an assessment of the threat posed by each country, the cost of implementation across the regulated sector and the potential unintended consequences.

As a starting point, a more proportionate, risk-based approach would be reflected if the drafting under Reg 33(3A) stated "the enhanced due diligence measures taken by a relevant person for the purpose of paragraph (1)(b) may include" rather than "must include."

Additionally, recent guidance received from the FCA to a trade association regarding HRTCs indicated the FCA's view that Regulation 33(1)(b) does not have retrospective application, i.e. the mandatory EDD only applies to customers onboarded at the time the country in which they are established is listed in Schedule 3ZA.

As a result, we believe the MLRs should be updated accordingly to reflect this, by replacing 33(1)(b) "in any" to "when establishing a business relationship:"

> *"b) when establishing a business relationship with a person established in a high-risk third country or in relation to any relevant transaction where either of the parties to the transaction is established in a high-risk third country."*

b. Enhanced Due Diligence for Politically Exposed Persons (PEPs)

PEP EDD measures are applied on the PEP if they are a customer in their own right, or a beneficial owner. The MLRs do not currently make it clear that the PEP EDD measures are not triggered in relation to deemed beneficial owners.

For example, if a client is a government entity/state owned entity (such as a central bank) there will inevitably be no BO, however the deemed BO will hold a prominent public function. Applying EDD in this low-risk relationship does not seem to be what was envisaged by these requirements.

Whilst the FCA guidance 2.40 on PEPs does allow firms to take an RBA to CDD/EDD for PEP BOs, the MLRs are silent on the matter, and should be updated for clarity.

We propose the MLRs are updated to align themselves towards the steer provided in the FCA guidance, that PEP EDD measures are not triggered in relation to deemed beneficial owners, and that this may be determined on an RBA.

c. Enhanced Due Diligence in HRTCs

The current approach with regards to the mandatory application of EDD for HRTCs does not result in a proportionate, risk-based response to the risks presented by activity in HRTCs. This is particularly demonstrated when considering the mandated application extra-territorially, within branches and subsidiaries themselves located in high-risk jurisdictions. This could be interpreted as all customers of branches or subsidiaries based in HRTCs required to be treated as high risk, bringing about concerns of operational viability and disproportionality, with low risk, legitimate customers being scrutinised regardless of the risk they pose to society.

The current obligation to apply EDD to domestic clients of HRTC generates an administrative burden, and takes the first and second lines of defence's focus away from the true high-risk clients. One bank noted a 1000% increase in cases in one of their overseas branches, since the mandated extra-territorial application obligation has been in place.

EDD measures should be commensurate to the client's risk profile, rather than being mandatory across the board, to avoid directing resources towards this low value activity.

We recommend the removal of mandatory EDD for branches and subsidiaries themselves based in HRTCs, in favour of a more proportionate risk focused approach, based on an individual determination basis.

d. Enhanced Due Diligence: Complex or unusually large transactions

EDD requirements have been extended from scenarios where transactions are "complex and unusually large" to those that are "complex or unusually large" under Regulation 33(1)(f).

Whilst it is reasonable to monitor a client that has been flagged by the system as undertaking an unusual transaction, it can generate unnecessary workload, especially in the scenario that this transaction is a unique event with a reasonable explanation.

It would be more effective to apply enhanced monitoring when the complex or unusually large transactions are detected on the same client for a second event, becoming repetitive behaviour, which would then trigger enhanced monitoring for a given timeframe to ensure there is no suspicious activity.

Further, as the objective meaning of the term “complex” is challenging to establish (anything in the financial services sector could arguably be considered “complex” by an individual in a non-banking profession), the common-sense interpretation of the term “complex or unusually large” is such that a “complex” transaction in the sense of Regulation 33(1)(f) is in fact already treated as “unusually complex”, we would suggest amending the phrase “complex or unusually large” to “unusually complex or unusually large” to make explicit this reasonable interpretation.

e. Correspondent Trading Relationships

There is limited value in automatically applying EDD on principal-to-principal correspondent trading relationships, where there is limited risk mitigation for added administrative burdens. EDD should be limited to scenarios where the respondent’s relationship with the firm is used to facilitate activity for their underlying customers, or where customer risk in the principal-to-principal relationship is assessed by the firm as high.

This is distinct from the amendment introduced last summer, clarifying that the requirement to perform EDD on the grounds of non-UK correspondent relationships applies to firms with correspondent relationships involving the execution of payments. This would be a further relaxation, for where there is a principal-to-principal relationship.

To align this requirement back to the risks, we recommend relaxation of the EDD application, so that correspondent trading relationships are only triggered when a financial institution is acting as an intermediary for their underlying customers and involving the execution of payments.

Furthermore, we would like to clarify with HMT the below:

- Clarification regarding intended definition of “third country” under Regulation 34(1);
- Introduction of a definition for “involving the execution of payments” for correspondent trading relationships under Regulation 34; and
- Clarity regarding the wider definition of correspondent relationship, considering Correspondent Banking Relationship (which is a product), Correspondent Trading Relationship and Correspondent Securities Relationship all differ, and clarity regarding the risks posed and the level of due diligence required for each.

2. Correspondent Banking Relationship definition

Currently not all actors, including new entrants, that offer services akin to correspondent banking are being picked up by the definition of correspondent banking relationship.

We believe the definition of correspondent banking relationship should be broadened, to reflect the increase in Non-Bank Financial Institutions and FinTechs who are now offering services without the formal regulatory oversight.

We request the same rules for all parties through the broadening of this definition, to ensure that all new entrants within the perimeter are required to comply with these requirements. This would not include third country AISPs as they are not involved in the execution of payments.

3. Pooled Client Accounts

The MLRs 2007 automatically offered pooled client accounts SDD application by banks. The MLRs 2017 updated Regulation 37(5)(a) to require pooled client accounts to be subject to SDD only where business relationships are deemed low risk. However, the MLRs do not define what due diligence measures can be applied to pooled client accounts.

This becomes particularly disproportionate for those customers that are not relevant persons under the MLRs, and are therefore deemed too low risk to require regulation, yet undergo stringent risk assessments to be able to continue operation of their pooled accounts.

The MLRs offer no explanation for what Standard or SDD means practically for pooled client accounts. This gap was previously filled by the EBA's guidelines, which are disproportionate, impractical and have resulted in the access to banking issues we have today. The production of updated JMLSG guidance has had limited practical impact because of the constraints of having to take account of the EBA's guidelines (EBA/GL/2021/02 section 9.16ff) of additional guidance, with sectors traditionally using client accounts, noting the more stringent risk requirements continue to impact the offering and availability of these accounts.

Whilst JMLSG has since been updated to provide clarity on the treatment of these accounts, members note that there has been limited practical impact of this additional guidance. This stems from the requirement to take account of the ESA guidance which greatly restricted use of SDD and introduced the requirement to treat all persons whose funds are held in the PCAs as beneficial owners.

Post-Brexit, some members would recommend consideration of realignment back to the requirements under MLRs 2007, to allow proportionate treatment of these accounts, and help alleviate access to banking concerns.

This would involve extending the use of SDD measures set by the ESAs beyond the very limited set of circumstances, with firms treating PCAs held by regulated firms in higher risk situations as 'light touch' correspondent relationships (i.e., banks will need to assess the customer's AML/CTF controls), linking into the conversation around monitoring or preventing risk from entering the system.

In relation to regulated sector entities who wish to access a pooled client account, we view the introduction of obligations to identify and verify underlying beneficiaries of funds in a pooled client account in the event of a relationship rated anything other than "low" risk as a strong indictment of professional body supervisors' capabilities. We would prefer to instead establish an approach that did not lead to UKF members essentially acting as a secondary supervisor for regulated sector entities.

If existing provisions are retained, consideration should be given to aligning the meaning of the term "persons on whose behalf monies are held" with the definition of "beneficial owners" in Regulation 5 to limit the severity of current obligations in any situation other than a low-risk relationship.

We would note that under the 4MLD, the 25% beneficial owner threshold was removed, meaning that all beneficiaries of a trust are beneficial owners, regardless of the materiality of their interest in the trust capital/income and regardless of whether they are discretionary or vested beneficiaries. Again, as above, the review of the MLRs post-Brexit is an opportunity to review the position which is currently driving low impact activity (Regulation 6.1c).

4. Treatment of Politically Exposed Persons

There are a number of instances, listed below, where inconsistencies between the approach set out between the FCA's guidance on PEPs, the FCA's SYSC guidance and the MLRs is causing confusion and fuelling low value activity across industry. It is entirely detrimental for guidance to be published that contradicts or differs from other guidance or regulations, as the resulting confusion and lack of clarity has huge practical impact on financial institutions.

We believe that the existing guidance documents should be revised, and aligned back to the MLRs, to promote a harmonised understanding of obligations across industry

a. Disproportionate regulatory expectations to domestic PEPs

There is tension between different regulatory expectations relating to domestic PEPs. Banks are expected to obtain MLRO sign-off for lower risk PEPS, as per FCA Guidance, but this is at odds with the requirements of the FCA Handbook. SYSC 6.3.9 requires the MLRO to have oversight over all areas of systems and controls against money laundering; it follows that the MLRO cannot (under SYSC 6.1.4(3)) be part of an operational process within that system and control framework as the FCA Guidance requires. Further, the FCA guidance says that domestic PEPs should not be specifically reported on via annual FCA REP-CRIM obligations.

There is a disconnect between the seniority of the level of sign-off required against the decision of the FCA not to require firms to specifically report domestic PEPs, and the legislative obligation to obtain "senior management", not necessarily MLRO approval.

b. Tensions between the FCA's guidance on PEPs[7] (FCA guidance) and SYSC guidance

FCA guidance defines MLRO approval as the minimum requirement for oversight and approval of lower risk PEPs (para 2.35), which is in direct tension with the FCA's SYSC 6.1.4(3) prohibition on relevant persons involved in the compliance function being involved in the performance of the services or activities that they monitor.

c. PEP relationship definitions

FCA guidance 2.21- 2.23 appears to go further than the 2017 MLRs, by stating that the PEP relationships listed are not exhaustive and contain brothers and sisters of PEPs, as well as a further reference to aunts and uncles being potentially included for higher risk PEPs. Further clarity is required around why these specific relations were called out beyond the scope of the 2017 MLRs, and which further relations would fall into scope.

d. Potential tension between FOS complaints and FCA guidance

The FOS has been granted jurisdiction for complaints from individuals who consider that they have been disadvantaged by misidentification as a PEP or by disproportionate treatment following correct identification as a PEP. Complaints of alleged misidentification as PEPs could be fuelled by the lack of clarity within the FCA guidance to begin with (e.g. family members).

e. International implications

[7] FG17/6: The treatment of politically exposed persons for anti-money laundering purposes

FCA guidance includes criteria for lower and higher risk PEPs, but we consider that some of this criteria is not straight forward to apply outside of the UK. For example, in jurisdictions such as China, the equivalent title to MP produces results in the thousands, often with no significant influence or exposure to grand corruption risk.

5. Treatment of Domestic PEPs

In addition to the points above, any review of PEP obligations needs to give mind to introducing a true risk-based assessment of PEPs, outside of mandatory EDD, that allows for a more tailored approach to individual scenarios.

A risk-based assessment of PEPs would be further enhanced by introducing a more nuanced approach to the treatment of domestic vs. foreign PEPs, in order to reflect the differing risk profiles presented. This amended approach would bring this approach in line with FATF Recommendation 12.

There should be enough flexibility introduced to allow for a true risk-based assessment of a PEP's susceptibility to corruption, and the measures in place to prevent it. This would allow low risk instances, such as serving UK politicians, to not have to face disproportionate EDD measures. However, this would also ensure that in the presence of additional risk factors, scrutiny could be increased accordingly, and would allow for a tailored assessment based on the risks presented by an individual customer.

This supports the discussions set out in the Call for Evidence response, around the drive for effectiveness. The cost to industry of conducting mandatory EDD on domestic PEPs far outweighs any AML/CTF benefit, as demonstrated by the absence of any prosecutions of domestic PEPs for grand corruption.

We believe this should be built into any revised PEP guidance, and the relevant flexibility reflected within the MLRs.

6. Beneficial ownership

a. BO vs PSC definition changes

There remains a misalignment between the definition of Beneficial Owner under the MLRs and People with Significant Control (PSCs), and the registration requirements for PSCs which may include legal entities and not a natural person/individual.

Alongside the lack of clarity introduced, these conflicting definitions in turn generate unnecessary discrepancy reporting obligations, draining resources that could be applied to higher priority areas of compliance.

The definition of PSC should therefore be aligned to that of Beneficial Owner.

b. Controlling Information

The current MLR approach duplicates the fit and proper person due diligence and controls as part of the licensing processes undertaken by the regulator.

It would be helpful to introduce a risk-based approach to SDD when determining beneficial ownership controlling information for financial institutions regulated in equivalent jurisdictions.

c. Regulation 5

The reference to “significant control” under Regulation 5 could be tightened, as it is not referenced elsewhere within the MLRs.

It would be useful to reiterate this under Regulation 28 and other CDD measure regulations, to make the treatment of significant controllers vs beneficial owners clearer.

7. Record Keeping

The existing requirements regarding record keeping within the MLRs deviate from FATF requirements, by going further than required.

Regulatory requirements to retain customer identification documents and supporting records, for 5 years from the date the customer relationship has ended, have been in place since the Data Protection Act (DPA) came into force in 1998. However, the DPA states that data should not be kept for longer than is necessary for the purpose it was intended.

Both the DPA requirements, and core MLR 2017 requirements, follow FATF Recommendation 10, which states that regulated firms should retain all necessary KYC records for at least 5 years after the business relationship or occasional transaction has ended. The MLRs also follow FATF Recommendation 10 in only requiring records of transactions within a business relationship to be retained for at least 5 years after the transaction.

4MLD departed from FATF standards in requiring deletion of personal data after a defined retention period. This rigid requirement for deletion is also in tension with GDPR, which is more flexible. 4MLD also departed from FATF standards in requiring retention of records of transactions within a business relationship for at least 5 years after the end of the business relationship.

The MLRs 2017 added the undernoted requirements:

- In addition to retaining customer identification documents, firms must have sufficient supporting records to enable transactions to be reconstructed (whether occasional transactions or transactions within a business relationship).
- 5 years after the business relationship has come to an end, any personal data contained in the records must be deleted.
- 5 years after an occasional transaction is complete, any personal data contained in the records must be deleted.

The MLRs 2017 also introduced the following exceptions to the defined data deletion periods:

- Transaction records only need to be kept for a maximum of 10 years from the date on which they are executed however there is no requirement to delete them after 10 years.
- Records required under another enactment.
- Records required for any court proceedings, or reasonable belief that they will be so required in future.

We believe realignment of requirements back to FATF Recommendation 10 are required, by neither requiring deletion 5 years after the end of the business relationship, nor requiring retention of transaction data indefinitely for ongoing business relationships. This would support wider discussions being held with the ICO as part of the DCMS review of data privacy regime.

Further clarity on what is meant in practice by “end of business relationship” and guidance on record retention where the customer has relationships with different “relevant persons” within a group would also be welcome.

8. Acting on Behalf Of (AOBO)

There is a lack of clarity regarding the scope of the Acting on Behalf Of requirements introduced under Regulation 28(10).

This breadth of the wording here could allow for certain scenarios to fall into scope that appear to be outside of the intended purpose of this provision.

We recommend that clarity is introduced regarding the intended scope of the AOBO provisions introduced under Reg 28(10).

9. Definition of Tax Advisor

The MLRs provide a definition of "tax adviser" under Regulation 11(d). However, this is very broad and could be read as including incidental services (for example, the provision of software that helps customers determine their tax liability). In particular, it includes the wording "assistance...in connection with tax affairs of other persons whether provided directly or through a third party".

This introduces a very broad definition, and one that brings into scope a broader range of tax advisor services than we believe were intended by these provisions.

We recommend the introduction of clarity around the scope of this provision, in particular to confirm whether it is the intention of the regulations to capture those providing software to help individuals to determine their tax liability.

10. Regulated Markets

The regulations have expanded the obligation to publish a simplified prospectus also to SME Growth Markets under Regulation 3.

With the MLRs specifically referring to the disclosure requirements for the Growth Market, it is unclear whether this impacts the categories of stock exchanges which can be considered as Regulated Markets.

We encourage clarity around this requirement, to confirm whether the changes impact the categories of stock exchanges considered Regulated Markets.

11. Legal Duty

Following changes to Reg 27(8), firms must apply CDD measures when they must contact an existing customer in order to fulfil any duty under the International Tax Compliance Regulations 2015 (e.g. FATCA, CRS, DAC2).

There is a lack of understanding of when legal duty triggers the obligation to review Client’s due diligence information and to what extent. In particular, there is a lack of understanding of whether obliged entities are mandated to engage with the client directly to fulfil these obligations, as in some

scenarios there may not be a need to engage with the client because their information might be available through third party vendors, or reliable public sources.

We request clarification on when the obligation to review due diligence is triggered, the process to engage clients, and the CDD measures applied.

12. Trusts Registration Service

Following publication of the Trusts Registration Service SI, there are a number of outstanding questions regarding clarity of obligations that remain unanswered.

Regarding the reporting of ultimate beneficial owner discrepancies to the trusts register, there is currently no guidance, mechanism, or access to the register in order to check and report discrepancies. There is also no understanding of details regarding expectations of extra-territorial application of trust beneficial ownership discrepancy reporting obligations, registration requirements, definition of a discrepancy, the process of discrepancy reporting alongside other practical considerations.

We encourage the production of guidance from HMRC to clarify these outstanding questions regarding the practical implementation of trust registration service obligations.

13. Further areas of the MLRs requiring clarity

There are additional areas of the MLRs where we believe the regulations, and subsequent successful practical implementation of regulations, would benefit from additional clarity. These include:

- Introduction of a definition of “business relationship” under Regulation 4(1);
- Clarification regarding intended definition of “ultimate control” under Regulation 5(1)(a);

14. Bank Account Portal

This Statutory Instrument consultation does not reference the removal of the requirements relating to the implementation of the Bank Account Portal. Since the HM Treasury confirmation that the UK will not be proceeding with introducing this requirement, the relevant provisions introduced under Part 5A should be removed accordingly for regulatory clarity.

ANNEX B

Other Obliged entities - Telecommunication and Social Media Companies

As part of considering the specific questions posed in the Consultation, our members have identified two additional sectors, telecommunications and social media, which are not currently obliged entities, but we consider users pose financial crime risks.

We believe that these sectors should also be considered, either as obliged entities or as otherwise incentivised to contribute to the UK's wider integrity and security regime. We have summarised below the elements of the existing framework which we consider to be relevant to these sectors.

A. General

- We believe that law enforcement should be able to give take-down or keep-open notices to social media and Telecoms companies, as they have in respect of transactions or bank accounts. We consider that the government should take the opportunity of new legislation to ensure that law enforcement have the powers they need to ensure all key sectors assist with law enforcement investigations and prosecutions.
- We consider that Ofcom's regulatory remit should be extended to include social media and internet service providers (ISPs) (as these are also communications channels). We also consider that their current consumer protection remit should be extended to incorporate financial crime prevention (we provide specific suggestions below of areas requiring regulatory attention).

B. Social media companies

- We consider that the use of social media companies, including ISPs, pose financial crime risks due to the multiple ways in which they are currently abused to enable and facilitate financial crime. For example:
    - Grooming for terrorism;
    - Advertising for money mules (commercially motivated);
    - Sales of stolen identity data and card data, including the prevalence of public sales sites on the Internet (as opposed to just the dark or deep web);
    - Inconsistent monitoring and identification of those at risk of grooming or performing lone wolf attacks to assist law enforcement with prevention measures, such as through relevant typology data and material changes in their search activity. Regulated firms monitor for equivalent behavioural change in financial transactions, which can trigger red flags for SAR consideration;

C. Telecommunication companies (Telcos)

- We believe that if Telcos, including mobile telephone service providers, mobile telephone retailers and SIM retailers, pose high financial crime risks due to the multiple ways in which they are currently abused to enable and facilitate financial crime. For example:
    - Many criminals use techniques such as SIM swaps or number spoofing to circumvent the controls in place at financial services firms. For example, they will apply to a mobile telephone company for a duplicate SIM which will then enable them to circumvent the callback or text confirm procedures of banks for unusual transactions on their customers' accounts. The president of the Communications Fraud Control Association acknowledged following publication of its 2017 Global Fraud Loss Survey:
        - "*Many services now utilise the mobile phone as the contact point for verification, whether this is to receive a call to verify a transaction or a text message with a one-time passcode or authorisation code. The mobile account of a consumer has become fundamental as part of an authentication trail in many services such as*

banking. Fraudsters therefore target customers accounts in order not to defraud the telecoms company but actually target the consumer themselves in order to manipulate their financial or other services."[8]

- Where multiple SIMs being used on the same device or from the same location, this can indicate organised crime SIM swap activity. It is not clear what controls Telcos have in place to mitigate the risk of insider-fraud (e.g., in mobile stores where such SIMs etc. can be authorised for use by organised criminals, or the risk of call-centre staff being socially engineered to give such authorisations).
- It is also not clear whether Telcos implementing new services or systems give explicit consideration of financial crime risk. For example, we are aware of continuing technical vulnerabilities of some mobile phones and some landlines to "keep line open" fraud attacks on their customers (e.g., where the criminal phones the customer with a scam designed to encourage them to phone their bank after the call and is then able to keep the line open so that they can hear the security answers provided by the customer when they do then phone their bank). We also consider that remote device takeover is a continuing vulnerability (e.g., where organised criminals contact the customer and pretend to need access to the mobile device in order to run security checks on the device).

There are also inconsistencies in how Telcos take account of typology data provided to them by banks (e.g., where Telcos have been alerted by banks to the exploitation of vulnerabilities in their devices and specific cases of abuse by organised criminals to commit crimes in mainstream financial services). This inconsistency can lead to cases where such vulnerabilities have been left open to exploitation for material periods after the sharing of alerts.

[8] https://www.thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807.

ANNEX C

Canadian e-ID model

The Canadian "Proceeds of Crime, Money Laundering, Terrorist Financing Regulations 2002-184" illustrate how their approach to e-ID permits CDD reliance on government verification. It permits the ability to rely on other local banks and Government Agencies (captured under section 5 of the act) who have already verified the identify of a customer.

The relevant legislation is copied below:

Proceeds of Crime, Money Laundering, Terrorist Financing Regulations 2002-184:

> **107 (1)** A person or entity that is required to verify a person's identity in accordance with subsection 105(1) may rely on measures that were previously taken by another person or entity if
>
> - **(a)** the other person or entity is referred to in section 5 of the Act;

In order to rely, under subsection (1), on measures taken by another person or entity, the person or entity that is required to verify a person's identity shall

- **(a)** as soon as feasible, obtain from the other person or entity the information that was confirmed as being that of the person and be satisfied that the information is valid and current and that the other person or entity verified the person's identity in the manner described in one of paragraphs 105(1)(a) to (d) or, if the measures were taken before the coming into force of this section, that the other person or entity ascertained the person's identity in accordance with these Regulations, as they read at the time the measures were taken; and
- **(b)** have a written agreement or arrangement with the other person or entity that requires the other person or entity to provide them on request, as soon as feasible, with all of the information that the other person or entity referred to in order to verify the person's identity.

> **108** A person or entity that is required to verify a person's identity under these Regulations shall keep a record that sets out the person's name and the following information:
>
> - **(i)** if, in accordance with subsection 107(1), the person or entity relied on measures taken by another person or entity, all of the information that is provided to them under paragraph 107(3)(b).