HM Treasury

Improving the effectiveness of the Money Laundering Regulations

Consultation

February 2024

Improving the effectiveness of the Money Laundering Regulations

This publication is available at: www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at: anti-moneylaunderingbranch@hmtreasury.gov.uk

ISBN: 978-1-916693-89-0 PU: 3401

Table of Contents

Ministerial Foreword

The UK's Money Laundering Regulations (MLRs) form a vital bulwark against the proceeds of crime entering the UK financial system. With new technologies being developed and continuing global threat from economic crime and illicit finance, it is more important than ever that we give businesses the right tools to identify and prevent money laundering and terrorist financing.

A balanced and effective AML/CTF (anti-money laundering and counter-terrorist financing) regime protects the UK's reputation as a modern, safe place to do business, and protects the integrity of the financial system. As a global issue, it is crucial that the UK continues to show leadership on economic crime, driving up standards worldwide and involving the private sector as an active partner.

Ultimately, it is important that our regulation and business environment is attractive to investors and supports economic growth. Smarter Regulation is fundamentally about ensuring that all areas of UK regulation work as well as they can, where regulation is needed. This includes minimising regulatory burden and future proofing regulations, making regulation a last resort and not a first choice, and ensuring a well-functioning landscape of regulators that are responsive and accountable. This shift allows tailored policies, better aligning with the UK's financial and economic landscape.

As the 2022 review of the UK's AML/CTF regulatory and supervisory regime and the Economic Crime Plan 2023-26 set out, there is always room to improve the effectiveness of the regime, especially in context of an evolving threat.

A key principle in the MLRs is proportionality. Where there is room to find a better balance between what we ask of regulated firms and customers, and the risk of money laundering and terrorist financing, then we want to seek to address this.

This consultation also focuses on areas of the MLRs where additional clarity might support compliance with the regime or where there might be opportunities for stakeholders to work together in a better way. It is right that we consider a range of ways of resolving these issues and invite the views of those involved or affected by the regime, before making changes. In parallel, we are launching a survey on the cost of compliance with the MLRs which will help inform our assessment of the impact of any changes proposed to the legislation.

Of course, the MLRs can only be effective alongside a robust supervisory regime to support compliance. In 2023, we launched a consultation on reforms to the AML/CTF supervision regime, following evidence that there remain weaknesses in its current format. We are currently

considering the responses to that consultation and expect to make decisions about the future of the system in the coming months. It is my intention that any amendments to the provisions in the MLRs will be supported by an improved supervision regime, further strengthening the UK's overall regime for reducing economic crime.

Baroness Vere

Executive Summary

This consultation aims to improve the effectiveness of the Money Laundering Regulations 2017 (MLRs), which place requirements onto a range of businesses in order to prevent money laundering (ML) and terrorist financing (TF). The consultation covers four core themes by chapter:

1. making customer due diligence more proportionate and effective
2. strengthening system coordination
3. providing clarity on scope of the MLRs
4. reforming registration requirements for the Trust Registration Service.

Chapter 1 focuses on the customer due diligence (CDD) requirements in the MLRs, including enhanced and simplified checks. This chapter explores some of the key stakeholder concerns about the proportionality of due diligence and various options to use the MLRs to achieve a better balance and support efforts to prioritise resource where it will have greatest impact. The chapter considers:

- whether the triggers for due diligence are sufficiently appropriate and clear, particularly for regulated firms that are not in the financial sector
- whether clarity can be provided to regulated firms on when to carry out 'source of funds' checks
- whether the requirement to verify anyone 'acting on behalf of' a customer is clear enough
- how best to support the use of digital identity when verifying customer identity
- ways to support firms' approach to the timing of CDD in cases of bank insolvency
- when enhanced due diligence checks (EDD) should be required
- if changes could be made to improve the proportionality and effectiveness of EDD in relation to High Risk Third Countries (HRTC)
- what steps could be taken to improve access to Pooled Client Accounts for unregulated firms.

Chapter 2 explores a number of issues that are intended to strengthen system coordination across the UK's AML/CTF regime. The proposed changes in this chapter reflect in part the need to update the MLRs, to ensure continuing effective cooperation as the system evolves to take account of new and emerging threats, technological change, and changes in the legislative landscape such as the Economic Crime and Corporate Transparency Act 2023. Chapter 2 also builds on the actions on this theme being taken forward as part of the Economic Crime Plan 2023-26 including commitments relating to system prioritisation. This chapter considers:

- ways to ensure that key information sharing and collaboration gateways are open and useful
- whether Companies House should be added to the list of bodies with whom AML supervisors must cooperate
- how regulated firms should use the National Risk Assessment of Money Laundering and Terrorist Financing (NRA) to help target their compliance work.

Chapter 3 explores issues that relate to the boundary of the AML/CTF regulation regime. This boundary and the guidance that supports firms and supervisors to comply with the regime needs to be kept updated, to keep pace with wider regulatory and market changes, following the UK's exit from the EU. This chapter considers:

- How the thresholds in the MLRs which are currently listed in euros could be changed to pound sterling;
- Potential gaps in the regulation of Trust Company and Service Providers (TCSPs);
- How best to align registration and change in control (CiC) measures for custodial wallet providers and cryptoasset exchange providers between the Financial Services and Markets Act 2000 and the MLRs.

Chapter 4 considers a range of potential changes to the registration requirements for the Trust Registration Service (TRS), which are given effect in the MLRs. The proposed amendments are intended to increase transparency in relation to certain higher risk trusts whilst reducing administrative burdens on low-risk trusts. Chapter 4 sets out proposals to do the following in relation to the TRS:

- include the registration of non-UK trusts, with no UK trustees that acquired UK land before 6th October 2020
- simplify trusts registration for estates management by aligning deadlines for certain trusts and removing the requirement to register from Scottish Survivorship Trusts

- introduce a de minimis for low-risk non-taxable trusts to reduce administrative burdens.

Background

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

The National Crime Agency (NCA) assesses that it is highly likely that over £12 billion of criminal cash is generated annually in the UK, with a realistic possibility that the scale of money laundering impacting on the UK is in the hundreds of billions of pounds annually.[1] . Money laundering and terrorist financing enables serious and organised crime which threatens the safety of individuals and communities in the UK and abroad. Unchecked, money laundering also risks the integrity and stability of global and UK financial markets and is a threat to the UK's national economic security and prosperity.

The UK's anti-money laundering (AML) and counter terrorist financing (CTF) regime seeks to identify and prevent money laundering (ML) and terrorist financing (TF), by placing requirements on financial institutions and the professional industries that are at higher risk of enabling illicit finance. Approximately 100,000 businesses are within scope of the regime, including banks, accountants, lawyers, estate agents, casinos and other sectors that are at high risk of being used for money laundering and terrorist financing purposes.

The UK has had an AML regime since 1994, and the current regime is set out in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs). The key requirements of the MLRs are:

- firms must carry out a risk assessment to identify and assess the risks of ML and TF to which the business is subject
- firms must (depending on size) appoint a nominated officer; screen relevant employees;, and establish an independent audit function to oversee the firm's compliance
- most firms must undergo Fit and Proper Checks on beneficial owners, officers and managers to screen for unspent criminal convictions for certain offences
- all new customers must be subject to both up-front and ongoing checks to 'know your customer' by verifying their

[1] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file

identity and assessing the purpose of the business relationship or occasional transaction

- high risk customers and transactions must be subject to Enhanced Due Diligence (EDD) measures, including to understand the source of the customer's wealth.

The MLRs are not prescriptive about how firms should meet these requirements. Instead, firms are required to take a 'risk-based approach' by adjusting their policies, controls and procedures according to the level of risk presented by a specific customer or transaction. The high-level nature of the requirements also reflects the variety of industries in scope of the MLRs. More detailed guidance on what constitutes effective arrangements for a particular sector is published by industry bodies or the supervisory and oversight bodies which oversee compliance with the MLRs across different sectors.

The MLRs have been amended several times since their introduction in 2017, using statutory powers under the Sanctions and Anti-Money Laundering Act 2018. The changes have aimed to reflect the evolving landscape of ML and TF risk, including new technologies such as cryptoassets, as well as to bring the MLRs in line with the latest international standards set by the Financial Action Task Force (FATF), an intergovernmental body which promotes effective implementation of measures for combatting money laundering and terrorist financing along with other threats to the integrity of the international financial system.

The 2022 Review of the Money Laundering Regulations, and the Economic Crime Plan 2023-26

In 2022, the government published a review[2] of the UK's AML/CTF regime (the '2022 Review') as well as a Post-Implementation Review of the MLRs. The review found that the MLRs work broadly as intended and continue to be in line with the international standards set by the FATF.

However, while the 2022 Review concluded that the risk-based approach at the heart of the MLRs remains appropriate, some weaknesses were identified in how they are implemented and enforced by the supervisory bodies. As a result, the government consulted on potential reforms to the UK's AML/CTF supervision regime in 2023. The conclusions of that consultation will be set out later this year.

The 2022 Review also identified some specific issues regarding how the MLRs are implemented by regulated firms, including in relation to

[2] https://www.gov.uk/government/publications/review-of-the-uks-amlcft-regulatory-and-supervisory-regime

providing access to 'pooled client accounts', applying EDD requirements, such as for customers or transactions established in High Risk Third Countries (HRTCs), and making use of Digital identity. The Review concluded that irrespective of the outcome of the consultation on supervision reform, changes to the MLRs in these areas had the potential to improve the effectiveness and proportionality of the regime. The government therefore committed to consult separately on options to address these issues.

The Economic Crime Plan 2023-2026 (ECP2)[3] sets out a holistic public-private partnership response to tackling economic crime, building on the foundations laid in the first Economic Crime Plan. ECP2 places a clear focus on achieving three tangible outcomes: reducing money laundering and recovering more criminal assets, combating kleptocracy and driving down sanctions evasion, and cutting fraud.

ECP2 includes a range of actions to tackle economic crime, including for HM Treasury to consult on a package of changes to improve the effectiveness of the MLRs (Action 6). While taking this forward, HM Treasury continues to deliver other actions aimed at reducing money laundering, including through its oversight of the public body AML/CTF supervisors (the Financial Conduct Authority, HMRC and the Gambling Commission).

Scope and themes of this consultation

Throughout the consultation we set out questions to invite input on options to address each issue. Not all options involve legislative change; we recognise that given the diversity of sectors covered by the MLRs, it may be more appropriate to address sector specific issues via guidance or engagement with supervisors.

We particularly welcome responses from civil society organisations and members of the public, as well as those directly affected by the regulations such as regulated businesses, sole traders, business associations, supervisors and law enforcement agencies.

Alongside the consultation we are also publishing a short survey on the current cost of compliance with the MLRs, which is aimed at businesses from across the regulated sector. The survey aims to enhance the government's understanding of the cost to businesses of meeting the different requirements under the MLRs, focusing particularly on staffing and customer due diligence costs. It will further help us to estimate the potential impact of the changes considered in this consultation.

[3] https://www.gov.uk/government/publications/economic-crime-plan-2023-to-2026

How to respond

- Our preferred format in which to receive responses is via HM Treasury's online Smart Survey form, which can be found here: https://www.smartsurvey.co.uk/s/6NIPPN/
- The separate survey referenced above on the cost of compliance with the MLRs can be found here: https://www.smartsurvey.co.uk/s/5MI1PN/
- Email responses should be sent to:

  Anti-MoneyLaunderingBranch@hmtreasury.gov.uk
- Questions or enquiries in relation to this consultation can also be sent to the above email address. Please include the words 'XX in your email subject. Whilst it is preferable to send responses electronically, if needed responses can be sent by post to:

  Sanctions and Illicit Finance Team (2nd Floor)

  HM Treasury

  1 Horse Guards Road

  London

  SW1A 2HQ

  London
- We encourage stakeholders to provide as much evidence as possible to help inform the government's response. Please include facts and figures where possible to justify your responses, including estimates of the impact of proposed changes on your business or sector. Additional comments are welcomed on the impact (negative, positive or neutral) of any proposed changes on individuals with protected characteristics[4] or the environment/climate. This will help us to assess the impact of any changes made and ensure evidence-based policy decisions.
- The consultation will remain open for three months. The closing date for responses to be submitted is Sunday 9 June 2024.
- Once the consultation has closed, the government will consider all responses and in due course publish a response outlining the next steps, including draft legislation if appropriate.

[4] https://www.gov.uk/discrimination-your-rights

Chapter 1: Making customer due diligence more proportionate and effective

Overview

1.1 Customer due diligence (CDD) is critical to a strong anti-money laundering/counter terrorist financing (AML/CTF) regime. Done effectively, due diligence means that businesses know their customers, verify their identities and develop a baseline for normal business with them against which they can identify unusual or suspicious transactions and activity. CDD under the Money Laundering Regulations 2017 (MLRs) is the first line of defence against money laundering and terrorist financing in the UK and generates an invaluable pipeline of intelligence for law enforcement via Suspicious Activity Reports (SARs), as well as deterring criminals from attempting to launder the proceeds of crime through regulated firms.

1.2 Engagement with the regulated sector, representative bodies and the public shows that some find the way in which due diligence requirements are applied to be burdensome or who feel the requirements lack purpose. Regulated industries often report that performing customer due diligence checks and on-going monitoring is expensive. Some firms consider that certain requirements are not useful or effective at identifying money laundering or terrorist financing. There is also a suggestion that some firms may choose to over-comply, by taking a blanket or overly risk-averse approach, for fear of falling foul of the law or supervisory expectations. In addition, consumer feedback indicates that customers often feel that checks are intrusive, administration-heavy or don't reflect their understanding of the risks they pose.

1.3 The risk-based approach, which runs throughout the MLRs, can be used to mitigate the above concerns. The MLRs require that firms take steps to assess the potential ML/TF risks in their sector and the differing levels of risk posed by their customer base. With this knowledge, firms must, within the limits set by the MLRs, apply due diligence checks which are commensurate to that understanding of the potential risk of a specific customer or business relationship. We continue to favour the risk-based

approach because it ensures regulated firms understand potential risks and requires them to carry out checks in a proportionate manner, minimising the impact on legitimate customers. This approach is also central to the international standards set by the FATF and in line with the regimes set by our key international partners.

1.4 It is important, therefore, that firms understand how to apply a risk-based approach, on a case-by-case basis, making use of the discretion permitted by the MLRs. There have been concerns raised that some firms may not feel confident flexing their approach to customer due diligence in line with the risk profile of a particular business relationship or managing the risk of more complex customers or those with risk factors which require enhanced checks. This, in turn, may contribute to certain individuals and businesses struggling to access financial or other services. One aim of this chapter is to understand this further.

1.5 The government's 2022 Review of the AML/CTF regulatory and supervisory regime covered aspects of the customer due diligence requirements in the MLRs, including enhanced due diligence, simplified due diligence and the requirements around reliance on due diligence carried out by a third party. The review focused on the ways these requirements relate to the risk-based approach.

1.6 The 2022 Review found that, in the main, the customer due diligence requirements in the MLRs continue to be the right ones. HMT set out that it was not minded to shift the balance of mandatory requirements under the MLRs except in some specific cases where a good case for considering regulatory change was identified. These included, for example: the mandatory checks for High Risk Third Countries (HRTCs) in regulation 33(3A); the requirement to perform enhanced due diligence on transactions that are complex or unusually large; and the approach to simplified due diligence on pooled client accounts. This chapter explores these issues in more detail and considers options for change.

1.7 The Financial Action Taskforce (FATF) standards shape the customer due diligence requirements of its member countries across the world. The standards provide an important basis for a robust and effective AML/CTF regime here in the UK, but don't preclude the MLRs from also reflecting the specific context of regulated industries and risk in the UK. While previous revisions to the MLRs and the 2022 review sought to consider this in detail, this consultation also contains several proposals which could serve to tailor the MLRs to the UK risk and context even further. This Chapter considers potential changes to the CDD requirements, including provisions for simplified and enhanced due diligence (SDD and EDD), which could be helpful to achieve a better balance between the burden placed on customers and firms, and risk of ML/TF.

Due Diligence Requirements

1.8 The MLRs require that regulated firms carry out CDD checks when establishing a new business relationship, carrying out a high-value transaction, or at certain other points. Customer due diligence involves the regulated firm taking steps to verify their customer's identity (including beneficial ownership where the customer is a legal person, trust, company or similar legal arrangement) and assess the purpose and intended nature of the business relationship or transaction.

1.9 The checks that can be carried out by regulated firms to be satisfied of this information are not prescribed by the MLRs, but firms must apply due diligence measures in a way that reflects their understanding of the risk posed by that customer (the 'risk-based approach'). Firms are also required to conduct on-going monitoring of customers and their transactions and take steps to verify identities, source of funds or the purpose of transactions, if necessary. There are additional requirements which are specific to certain circumstances and certain regulated sectors.

1.10 The MLRs require that an enhanced level of customer due diligence and customer monitoring ('enhanced due diligence' or 'EDD') is applied where either the MLRs set out that a customer/transaction presents a higher risk of ML/TF or where the regulated firm determines this. The MLRs do not prescribe the EDD that should be carried out, except in some specific cases, such as in relation to High Risk Third Countries (HRTC) and for Politically Exposed Persons (PEPs), but require that firms take sufficient steps to manage and mitigate any additional risk identified.

1.11 Just as enhanced checks are required when risk is identified to be higher, where the ML/TF risk is identified as being low (on the basis of customer, transaction or geographical risk factors), simplified customer due diligence (SDD) can be applied. This means that the extent, timing or type of customer due diligence measures can be adjusted, although the core requirements of CDD must still be met in some form.

1.12 For all of the above due diligence types, the MLRs set out additional or varied requirements that are specific to certain types of customer and transactions.

Customer Due Diligence

1.13 This section covers the core customer due diligence measures required for all customers of regulated businesses under regulations 27 and 28 of the MLRs. Given their broad scope, these

measures have a significant impact on both regulated firms and their customers, who will be subject to due diligence for example when opening a bank account, purchasing property or instructing a solicitor.

1.14 The 2022 Review of the MLRs concluded that these requirements were broadly appropriate and effective at mitigating the risk of money laundering and terrorist financing. However, the government is keen to reduce any ambiguities in the requirements which could result in over-compliance or inconsistent application.

1.15 We would therefore like to consult on three issues where we understand there is a risk of ambiguity: the trigger points for when due diligence is required; the requirement for source of funds checks on customers; and the checks required where a person purports to act on behalf of a customer.

1.16 This section also explores two issues in relation to verification of customer identity, where the government is keen to encourage the use of digital identities, as well as to consider the case for more flexibility in exceptional circumstances such as bank insolvency.

Due diligence triggers for non-financial firms

1.17 It is essential that regulated businesses understand the points at which they need to apply customer due diligence under the MLRs, and that the MLRs are drafted in a way which works for all relevant persons, including non-financial firms.

1.18 Regulation 27 of the MLRs sets out the 'trigger' points at which regulated firms must undertake customer due diligence. The primary triggers, which are applicable to all regulated sectors, are set out at paragraphs (1) and (2) as follows:

- when the firm establishes a business relationship (which is defined in regulation 4)
- when the firm carries out an occasional transaction that amounts to a 'transfer of funds' exceeding 1,000 euros
- when the firm suspects money laundering or terrorist financing
- when the firm doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification
- when the firm carries out an occasional transaction that amounts to 15,000 euros or more (certain sectors are exempt from this trigger)

- various points in relation to existing customers, including if there is any change in the customer's identity or beneficial ownership.

1.19 There are also sector-specific triggers in relation to high value dealers, casinos, letting agents, art market participants, cryptoasset exchange providers, and custodian wallet providers. These take account of different patterns of risk in certain sectors, or reflect the particular ways in which business is done in these sectors.

1.20 We would like to consult on whether the primary triggers set out at regulation 27(1) and (2) are sufficiently clear and easy to apply, particularly as they relate to non-financial sectors. If the triggers are ambiguous or difficult to apply in certain contexts, we will consider whether amendments are necessary to provide clarity, or potentially the introduction of additional sector-specific triggers. We would welcome suggestions as to how the triggers in Regulation 27 could be more clearly drafted.

1.21 For instance, we recognise that the precise point at which a "business relationship" is established with a customer may be unclear in certain sectors. For this reason, Regulation 4 provides additional detail on the meaning of "business relationship", including sector-specific definitions for estate agents and trust or company service providers. However, we would like to understand if further clarity on the meaning of this trigger would be helpful.

1.22 We are not at this stage considering the appropriateness of the financial thresholds in regulation 27. This is because, as set out in Chapter 3 below, the right vehicle through which to assess the risk level in different sectors is the National Risk Assessment of Money Laundering and Terrorist Financing (NRA). However, we are consulting at this stage on whether the thresholds should be expressed in euros or sterling (also see Chapter 3).

Q1 Are the customer due diligence triggers in regulation 27 sufficiently clear?

Source of funds checks

1.23 Regulation 28(11)(a) sets out that, as part of the ongoing monitoring of a business relationship, the relevant person should scrutinise 'transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, the customer's business and risk profile.' While the legislation doesn't set out specific scenarios or time periods where a source of funds check is required, the intent of the provision is clear that such a check can be used to assure the relevant person that ongoing transactions are consistent with their knowledge of the customer.

1.24 We understand that some firms would like more clarity about regulation 28(11)(a) and, potentially, to be provided with specific scenarios in which a source of funds check might be applied. We do not think that amending the law to include specific examples of when source of funds checks under regulation 28(11)(a) is required. Our view is that this could create unnecessary or unhelpful (in establishing risk) mandatory checks. Inserting a list of scenarios, even if not mandatory, is unlikely to be comprehensive and risks being quickly outdated. It is our view that the regulation should continue to allow the relevant person to apply such a check where it is necessary, based on **their** understanding of their sector, customer base and whether such a check would help them establish the relevant level of risk.

1.25 The guidance produced by the Joint Money Laundering Steering Group (JMLSG) sets out a number of scenarios where enquiries into a customer's source of funds might be relevant or appropriate. The guidance produced by the Legal and Accountancy Professional Body Supervisors (PBS) affinity groups likewise cover this provision, albeit to varied degrees. We would like to understand whether more, or more detailed, sector-specific guidance on the potential for source of funds checks under regulation 28(11)(a) could be helpful to firms in particular parts of the regulated sector and what this might look like in practice.

Q2 In your view, is additional guidance or detail needed to help firms understand when to carry out 'source of funds' checks under regulation 28(11)(a)? If so, in what form would this guidance be most helpful?

Verifying whether someone is acting on behalf of a customer

1.26 Regulation 28(10) stipulates that where a person purports to act on behalf of the customer, regulated firms must verify that the person is authorised to act on the customer's behalf, and establish and verify the person's identity on the basis of documents or information obtained from a reliable source which is independent of both the person and the customer.

1.27 This provision provides an important safeguard against fraud and misuse of accounts, which can be carried out by individuals falsely claiming to act on behalf of a customer. However, we would like to consult on whether the language used in regulation 28(10) is sufficiently clear. We understand from engagement with financial sector bodies that there may be confusion among regulated firms over the scope of the 'acting on behalf of' requirements, for instance as regards how they apply when the customer or the person is a corporate entity. This may be resulting in firms treating a wider range of scenarios as falling under the requirements than

is necessary, creating additional burdens for both firms and customers.

Q3 Do you think the wording in regulation 28(10) on necessary due diligence on persons acting on behalf of a customer is sufficiently clear? If not, what could help provide further clarity?

Digital identity verification

1.28 Identity verification is an important step in ensuring that regulated firms know their customers and can identify those who may pose a high risk of money laundering or terrorist financing. Thorough and effective processes to verify the identity of customers can prevent the use of false or stolen identities, which is a common feature of certain types of economic crime.

1.29 For these reasons, verification of customer identity is a fundamental part of the customer due diligence measures required under the MLRs. However, the government recognises that identity verification can be complex and resource-intensive for regulated firms, and time-consuming for legitimate customers. The government is committed to considering ways to minimise the burden of identity verification for firms and customers while ensuring it remains effective at reducing the risk of ML/TF. This section considers issues related to digital identity verification through this lens.

1.30 A digital identity is a digital representation of you and facts about you. It lets you prove who you are during interactions and transactions. You can use it online or in person.

1.31 The government is committed to actively encouraging and realising the benefits of digital identity technologies in the UK, without creating or mandating identity cards. As part of the Data Protection and Digital Information (DPDI) Bill, we are now putting in place the necessary framework and tools for people to use digital identities confidently in an increasingly digital economy, if they choose to do so.

1.32 In collaboration with key organisations across the public and private sectors, the government recently updated its Good Practice Guide 45 (GPG45)[5], which helps individuals and businesses decide how to check someone's identity. Measures in the DPDI Bill build on our commitment to strengthen domestic

[5] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity

and international confidence in the UK's digital identity marketplace. They underpin the UK's digital identity and attributes trust framework (currently in its beta version), which sets out rules including roles, principles, policies, procedures and standards against which organisations can have their digital identity products and services certified.

Digital identity and the MLRs

1.33 As set out in ECP 2, the government will continue to engage with industry and civil society about the potential for digital identity technology to enhance our efforts to tackle economic crime. This includes the potential to reduce the burden of identity verification for firms and customers. For example, GOV.UK One Login[6] – a new single sign-in and digital identity solution for the whole of government – is making advanced identity proofing technologies readily available to public sector services. We are keen to continue making such progress more widely, beyond the public sector.

1.34 The MLRs are currently intended to be technology neutral with no preference between the use of digital identities or physical identity sources to verify customer identity. As set out in regulation 28(18), in this context, verifying a customer's identity means verifying that identity on the basis of documents or information 'obtained from a reliable source which is independent of the person whose identity is being verified'. Regulation 28(19) clarifies that an electric identification process may be used where such a process is "secure from fraud and misuse" as well as being "capable of providing assurance that the person claiming a particular identity is in fact the person with that identity, to a degree that is necessary for effectively mitigating any risks of ML/TF."

1.35 This means in line with the requirements of regulation 28 and the FATF's approach, digital source documents, data or information must be both reliable and independent, which means that any digital identity processes used should rely on technology and sufficient governance, processes and procedures to provide the appropriate levels of confidence that the system produces accurate results[7].

1.36 In the government's 2021 Call for Evidence on the UK's AML and CFT regime, we asked respondents a series of questions on

---

[6] https://www.sign-in.service.gov.uk/

[7] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-Executive-Summary.pdf

whether the MLRs, as currently drafted, are obstructing the wider adoption of technologies or digital identities and possible amendments to improve adoption of these innovations.

1.37 Respondents to the Call for Evidence signalled a desire for greater clarity with respect to which electronic identity verification processes satisfy the requirements of Regulation 28(19). In the 2022 Review, the government therefore stated it would consider amending the MLRs to ensure greater clarity on the status of electronic identity processes certified against the UK digital identity and attributes trust framework.

1.38 However, the government is aware that the MLRs are only one regulatory vehicle that influences industry's decision making and wider market adoption. Moreover, we recognise that digital identity assurance frameworks and standards and the MLRs have different purposes and intended audiences.

1.39 The government therefore considers it appropriate to first fully explore where and how additional guidance can empower industry and increase market confidence in digital identity before considering further regulatory interventions. As part of this explorative approach, the government is considering the value of producing bespoke guidance, explaining how regulated firms can refer to the UK digital identity and attributes trust framework, in relation to fulfilling their regulatory obligations under the MLRs. This guidance would clarify how the combined use of the trust framework, as a document of rules, standards and other requirements that apply to the whole economy, and GPG45 can facilitate reliable customer identity verification as required by the MLRs.

1.40 We would like to consult on what information should be included in any such guidance, and whether guidance published on GOV.UK is the right vehicle to provide clarity on the safe and effective use of digital identity technology in this context.

Q4 What information would you like to see included in published digital identity guidance, focused on the use of digital identities in meeting MLR requirements? Please include reference to the level of detail, sources or types of information to support your answer.

Q5 Do you currently accept digital identity when carrying out identity checks? Do you think comprehensive guidance will provide you with the confidence to accept digital identity, either more frequently, or at all?

Q6 Do you think the government should go further than issuing guidance on this issue? If so, what should we do?

Timing of verification of customer identity

1.41 Regulation 30(4) of the MLRs requires credit or financial institutions to implement "adequate safeguards" to ensure that they do not transact with or on behalf of new customers before verification of identity is complete. The government recognises that this requirement could lead to delays in circumstances in which banks are onboarding an unusually large volume of new customers.

1.42 One such circumstance, albeit rare, is in a bank insolvency. Where it is in the public interest to place a bank into insolvency, customers of the insolvent bank who do not have an alternative account may need to open accounts with other banks in order to maintain access to banking services (although it is important to note that this is not a necessary step to obtain compensation under the Financial Services Compensation Scheme, which protects eligible customers when authorised financial services firms fail). The insolvency of a bank with a large customer base could result in other banks receiving more applications for new accounts than they are able to process in a short period of time.

1.43 In this scenario, identity verification checks could add to delays for affected customers, who would not have access to banking services while the bank works through any due diligence backlog. This could affect both personal and business customers depending on the customer base of the insolvent bank.

1.44 While bank insolvency is rare in the UK, where it is in the public interest it is important that any disruption to depositors and the wider economy is minimised. Recent work led by the Bank of England on improving depositor outcomes in bank or building society insolvency identified several areas of work in support of this objective. These included exploring better operational support and capacity at receiving banks for those depositors who need to open a new bank account to achieve continuity, especially where there are challenges to opening a current account for the depositor. We would therefore like to seek views on how best to balance this objective with the need to ensure an appropriate level of due diligence is done on customers of banks and other regulated firms, while recognising that this is one of a range of issues associated with high-volume onboarding.

<u>Non-legislative approach</u>

1.45 Under a non-legislative approach, we would work with the Joint Money Laundering Steering Group and the Financial Conduct Authority to clarify in guidance how banks should approach the onboarding of customers from a failed bank within the MLRs as they stand. This might include exploring the potential for banks to make use of the provision on reliance in regulation 39 to rely on the due diligence done by the insolvent bank until the successor

bank is able to complete its own identity verification on the new customers.

Legislative approach

1.46 Under a legislative approach, we would amend the MLRs to provide for a limited carve-out from the requirement to ensure that no transactions are carried out by or on behalf of new customers before verification of identity is complete. This would be limited to scenarios in which a Bank or Building Society is placed into insolvency via the Bank/Building Society Insolvency Procedure, and potentially further limited to insolvencies which carry the potential for significant disruption. The amendment might still require banks to implement safeguards to prevent high risk transactions from taking place before the bank is able to complete identity verification. The amendment could also require the Financial Conduct Authority to set a reasonable expectation for timing and nature of completion of identity verification on a case-by-case basis, given that this will vary according to the circumstances of the insolvency.

Q7 Do you think a legislative approach is necessary to address the timing of verification of customer identity following a bank insolvency, or would a non-legislative approach be sufficient to clarify expectations?

Q8 Are there other scenarios apart from bank insolvency in which we should consider limited carve-outs from the requirement to ensure that no transactions are carried out by or on behalf of new customers before verification of identity is complete?

Enhanced Due Diligence

1.47 Where a customer or particular transaction or business relationship is assessed as having a higher risk of money laundering or terrorist financing, it is right that enhanced checks should be carried out. Firms can apply greater scrutiny and obtain more information about their customers, such as understanding the source of their funds, in order to better identify suspicious activity. The risk-based approach is intended to ensure that firms don't have to carry out an extensive list of enhanced checks on every customer; more detailed checks or specific checks only need to be carried out where a customer or transaction is identified as having higher risk factors, some of which are specified in regulation 33 of the MLRs.

1.48 The government wants to make sure that the triggers for EDD are still appropriate and that they support regulated persons to usefully identify higher risk customers or transactions, as they are experienced in the UK. In addition, the government wants to make

sure that firms can apply the risk-based approach when carrying out enhanced due diligence: that they aren't carrying out checks unnecessarily on customers which would otherwise be considered low risk and that they aren't carrying out specified checks which aren't helpful in identifying any suspicious behaviour in practice.

1.49 However, the government is clear that these checks must be applied in a proportionate and risk-based manner, reflecting Financial Conduct Authority (FCA) guidance. In legislation that came into force on 10 January 2024. The government recently clarified in legislation that under the MLRs the starting point for banks and other regulated firms in their treatment of domestic PEPs, or a family member or known close associate of a domestic PEP, must be to treat them as inherently lower risk than non-domestic PEPs. Accordingly, regulated firms must when assessing for EDD for a domestic PEP, start from the position that the level of risk associated is less than that for a non-domestic PEP, unless other risk factors are present.

1.50 Section 78 of Financial Services and Markets Act 2023 also committed the FCA to conduct, and publish the conclusions of, a review into how financial institutions are following its guidance. This review, underway separately to this consultation, is considering whether the FCA's guidance on PEPs remains appropriate, and the FCA will be required to amend its guidance if the review finds it necessary to do so. If the FCA finds that the guidance is no longer appropriate, it will publish draft revised guidance for consultation, taking into account the Treasury's amendment to the Regulations, within the 12-month timeframe given for the review (i.e., by 29 June 2024). Given the strength of concern on this issue, the Government expects that the FCA will continue to prioritise this important review over the coming months.

General triggers for enhanced due diligence

1.51 The majority of the risk factors that require enhanced due diligence to be carried out are derived from the FATF standards. These rightly point firms in the direction of customer, geographic, delivery channel, services, transaction and product risk factors. More specific factors, such as correspondent banking, new technologies, wire transfers, also appear in the FATF standards' coverage of enhanced due diligence.

1.52 There are a few areas where the UK has previously gone further than the FATF standards and therefore it is right that we consider whether this strikes an appropriate balance between mitigating risk and burdens on business, and what the evidence base tells us.

1.53 Regulation 33(6) sets out that, when a firm is assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, the following risk factors must be taken into account (amongst other factors, including any not listed):

- where 'the customer is the beneficiary of a life insurance policy'
- where 'the customer is a third country national applying for residence rights in or citizenship of a state in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities in that state'
- 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 rare scientific value'.

1.54 While we think it is right that regulated firms should be considering a range of customer and product risk factors, and that the specific factors above could indicate a higher-risk customer or transaction, it is not necessarily the case (or required by law) that every single customer or transaction with these specific factors must be subject to enhanced due diligence, only that the relevant person has considered the risks posed by these factors. However, we understand that some in the industry find the above risk factors are not relevant or useful to identifying suspicious activity. As such, we would like to better understand the impact of these requirements on regulated firms and their due diligence activities.

Q9 (If relevant to you) Have you ever identified suspicious activity through enhanced due diligence checks, as a result of the risk factors listed above? (Regulations 33(6)(a)(vii), 33(6)(a)(viii) and 33(6)(b)(vii)). Can you share any anonymised examples of this?

Q10 Do you think that any of the risk factors listed above should be retained in the MLRs?

Q11 Are there any <u>other</u> risk factors for enhanced due diligence, set out in regulation 33 of the MLRs, which you consider to be not useful at identifying suspicious behaviour?

Q12 In your view, are there any additional risk factors that could usefully be added to, for example, regulation 33, which might help firms identify suspicious activity?

'Complex or unusually large' transactions

1.55 Another risk factor, which requires regulated firms to carry out EDD, is where the relevant person identifies that 'a transaction is complex or unusually large.' The FATF's Recommendation 10 gave rise to this provision, with the interpretative notes setting out that:

Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified.[8]

1.56 When the MLRs were enacted, regulation 33(1)(f)(i) required that enhanced due diligence must be applied where 'a transaction is complex and unusually large'. In 2019, this was amended to where 'a transaction is complex or unusually large'. This change had the effect of widening the number of transactions that were captured.

1.57 We think that the general principle of applying enhanced checks or additional monitoring to customers who carry out complex or unusual transactions continues to be a reasonable requirement. Amongst other things, transactions which are complex increase the risk of information or activities being obscured (either purposefully or not) while unusual transactions (that is, compared to a customers' usual transaction types) could mean that the firm's initial understanding of the customer's risk level is no longer applicable and further steps should be taken to assess this.

1.58 As the 2022 review of the UK's AML/CTF regime set out, the requirement to apply enhanced due diligence to 'complex' transactions can be challenging. What constitutes a complex transaction differs between industries and across customer bases. For example, a transaction in one industry might appear 'complex' to others but the structure of the transaction might be relatively routine for that industry. Industries that have many such 'complex' transactions might find that they apply enhanced due diligence to most or every transaction. In addition, there have been suggestions that where a 'complex or unusually large' transaction has a reasonable explanation, the work carried out to reach that understanding was unnecessary.

1.59 The FATF standards do make it clear that a risk based approach should be used when applying enhanced due diligence and that any enhanced checks should be 'consistent with the risks identified'. This is also the intent of the provisions in the MLRs; other than where it is specifically set out, the expectation is that firms apply checks which 'manage and mitigate the risks' (Reg 33(1)). This means that firms should use their knowledge of their specific industry to identify only relevant transactions – for example those that are unusually complex, or which have other

8 https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf, p72

high-risk factors, or are so complex by their nature that the firm cannot be assured of the risk. We think that it is right that, where higher risks are identified, further steps are taken to ensure there is no suspicious activity. Some transactions and customers will be subject to checks which result in the firm finding no additional concerns. Without a requirement to carry out appropriate checks commensurate with the understood level of risk, suspicious activity could be concealed more easily.

1.60 We appreciate that the risk based approach, by its nature, can be challenging to apply and that concerns around non-compliance could lead to firms over complying. We are keen to understand how firms could be supported to apply the risk based approach to this provision and whether any of the more negative impacts of the provision can be understood and addressed.

Q13 In your view, are there occasions where the requirement to apply enhanced due diligence to 'complex or usually large' transactions results in enhanced due diligence being applied to a transaction which the relevant person is confident to be low-risk before carrying out the enhanced checks? Please provide any anonymised examples of this and indicate whether this is a common occurrence.

Q14 In your view, would additional guidance support understanding around the types of transactions that this provision applies to and how the risk-based approach should be used when carrying out enhanced check?

Q15 If regulation 33(1)(f) was amended from 'complex' to 'unusually complex' (e.g. a relevant person must apply enhanced due diligence where… 'a transaction is unusually complex or unusually large'):

- **in your view, would this provide clarity of intent and reduce concern about this provision? Please explain your response.**
- **in your view, would this create any problems or negative impacts?**

High Risk Third Countries

1.61 Responses to the last consultation on the Money Laundering Regulations and on-going engagement have made clear that some regulated firms find complying with the mandatory requirements for customers and transactions established in 'High Risk Third Countries' (HRTCs) to be expensive and burdensome. We recognise that this is particularly true for instance where firms have a large number of existing customers who are established in a country that becomes higher-risk, or where firms have branches and subsidiaries operating in such locations. At the same time, this

needs to be balanced with ensuring that there are effective measures in place to manage cross-border ML/ TF risks and ensure the UK complies with international standards set by the FATF.

1.62 The government wants to improve proportionality across the MLRs and find solutions which create a better balance between managing the risks associated with jurisdictions with weak AML/CTF regimes, and the cost of compliance to businesses. As part of this work, we have already legislated in January 2024 to improve the process and speed for us updating industry on changes to the list.

1.63 The FATF recommends that member countries mandate the application of EDD to customers and transactions established in countries on their 'Call to Action'[9] list. This is a list of countries with serious strategic deficiencies in their AML/CTF regimes (currently consisting of Iran, Myanmar and North Korea). The MLRs give effect to this requirement, and also require that EDD is applied to customers and transactions established in countries on the FATF's 'Increased Monitoring' list.[10] This is a list of countries identified through a mutual evaluation process as having strategic deficiencies in their AML/CTF regimes. The Increased Monitoring list currently contains 27 different countries.

1.64 The government's objective is to find a way to ease burdens on businesses, while maintaining compliance with the FATF standards and continuing to protect the UK from the threat posed by customers or transactions that relate to countries with weak AML/CTF regimes. This objective could be approached in a variety of ways and, as such, we want to understand how the HRTC requirements are viewed by different stakeholders and what would be the impact of any changes.

<u>The current rules for EDD in relation to HRTC</u>

1.65 **When EDD is required in relation to HRTC:** Regulation 33(1)(b) sets out that EDD and enhanced ongoing monitoring must be applied *'in any 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 transactions is established in a high-risk third country'.* Regulation(1)(g) also sets out that EDD and enhanced ongoing monitoring must be applied 'in any other case which by its nature can present a higher risk of money laundering or terrorist financing'. This latter requirement could cover,

---

[9] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2023.html

[10] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2023.html

amongst many other scenarios, other customers or transactions relating to other jurisdictions which could present a higher risk of ML/TF. Regulated firms must take a risk-based approach in identifying such jurisdictions, supported by sector-specific guidance published by the AML/CTF supervisors and cross-cutting guidance such as the NRA

1.66 **How EDD and enhanced ongoing monitoring must be carried out**: Regulation 33(3A) sets out a series of checks that the relevant person must carry out when applying EDD and enhanced ongoing monitoring in relation to a customer or transactions established in a HRTC. This must include, but is not limited to,: obtaining additional information on the customer and on the customer's beneficial owner, obtaining information on the source of funds and source of wealth of the customer; obtaining information of the reason for the transactions; conducting enhanced monitoring of the business relationship by increasing the number of timings of controls applied and selecting patterns of transactions that need further explanation. This list of checks is specific to HRTC customers/transactions and is not required for other customers subject to EDD, although similar sorts of checks might be applied using a risk-based approach.

1.67 **Existing customers:** When a new country is added to one of the two FATF lists, firms must carry out EDD on their existing customers established in those countries (as well as new customers and transactions). The government has already taken steps to clarify this expectation with supervisors and regulated firms. However, we appreciate that applying EDD to existing customers can be resource intensive where there are many existing customers falling into scope, even where a risk based approach is taken to the order and speed at which customers are checked at an enhanced level.

1.68 **Branches and subsidiaries:** Regulation 20 of the MLRs requires that regulated firms apply customer checks which are 'equivalent' to those set out in the MLRs in their overseas branches and subsidiaries. While the FATF standards also require that 'equivalent' checks are carried out at branches and subsidiaries, it is worth noting that the FATF is also clear that AML/CTF programmes should be 'appropriate to the business of the branches and...subsidiaries.[11] Where a firm has a branch or subsidiary operating in a HRTC, it may be the case that firms are applying EDD and enhanced ongoing monitoring to the entirety of their customer base or transactions at that location, to achieve this equivalence. We appreciate that this can be costly and may

[11] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf, p87

prevent firms from taking into account factors which may lower the risk posed by customers to the UK economy.

Supporting firms to take a more risk-based approach in relation to HRTC

1.69 **"How" firms carry out EDD:** The 2022 Review of the MLRs explored the idea of allowing firms to flex which enhanced checks are required for customers or transactions established in HRTCs. We think that requiring a risk based approach to EDD checks, instead of a mandatory set of checks, could helpfully ease much of the administrative burden without significantly reducing the valuable intelligence gathered through mandatory EDD (such as source of wealth information).

1.70 The mandatory checks listed at regulation 33(3A) are not all required by the FATF and, therefore, it may be possible to align the EDD requirements for HRTCs with other EDD triggers, by removing this prescriptive list or making it non-mandatory.

1.71 In this scenario, firms would still need to apply EDD and enhanced ongoing monitoring to HRTC customers and transactions, but could choose how they do this, and which checks they apply, in line with their understanding of the customer's risk profile and what is appropriate for the situation in question.

Q16 **Would removing the list of checks at regulation 33(3A), or making the list non-mandatory, reduce the current burdens (cost and time etc.) currently placed on regulated firms by the HRTC rules? How?**

Q17 **Can you see any issues or problems arising from the removal of regulation 33(3A) or making this list non-mandatory?**

1.72 **"When" firms carry out EDD:** While we think that the change to regulation 33(3A) set out above could better balance the AML/CTF controls relating to customers and transactions established in HRTCs and the burdens these create for regulated firms. We appreciate that some firms may think the proposals do not go far enough, and that it may be possible to make different changes to the MLRs to achieve this balance, while remaining compliant with the FATF standards. As set out above, while the current rules require EDD to be carried out on all customers/transactions established in countries on the FATF's 'Increased Monitoring' list and the 'Call to Action' list, the FATF only requires this in respect of the 'Call to Action' list. In addition, outside of reference to the HRTC list, regulation 33(6)(a)(ii) of the MLRs also requires that regulated firms take notice of geographical factors when assessing risk and deciding whether the risk is high enough to apply EDD.

Q18 **Are there any High Risk Third Country-established customers or transactions where you think the current requirement to**

carry out EDD is not proportionate to the risk they present? Please provide examples of these and indicate, where you can, whether this represents a significant proportion of customers/transactions.

Q19 If you answered yes to the above question, what changes, if any, could enable firms to take a more proportionate approach? What impact would this have?

Simplified Due Diligence

1.73 As part of the 2022 Review, the government considered whether the MLRs set out a proportionate and appropriate framework for the application of Simplified Due Diligence (SDD).

1.74 The MLRs explicitly permit regulated firms to vary the extent, timing and type of CDD measures they apply in low-risk situations, known as applying SDD. This does not provide an exemption from the core CDD requirements to verify the identity of each customer and understand the purpose of the relationship but encourages firms to consider less intrusive checks than they might normally undertake, in the absence of low risk factors.

1.75 For instance, depending on the circumstances, SDD might involve:

- verifying identity on the basis of one document only
- assuming the nature and purpose of the business relationship because the product is designed for one particular use only
- undertaking less frequent CDD updates and reviews of the business relationship relative to relationships presenting fewer high risk factors
- undertaking less frequent and lower-intensity monitoring of transactions relative to transactions presenting fewer high risk factors.

1.76 The 2022 Review concluded that despite low uptake of SDD by regulated firms, the provision made for SDD in regulation 37 of the MLRs was broadly appropriate, and that it was for sector-specific guidance to encourage better uptake by providing further examples of what SDD could involve or in which low risk situations it might be appropriate. For example, the above list of SDD practices is reflected in guidance for the financial sector published by the Joint Money Laundering Steering Group (JMLSG).

1.77 However, following further dialogue and engagement with supervisors and the regulated sector, we consider that there may be scope to expand the list of customer risk factors specified in regulation 37(3)(a), for the purposes of considering whether a particular situation represents a low risk of money laundering (ML)

and terrorist financing (TF), and therefore whether it would be appropriate to consider applying SDD. While not exhaustive, this list could be updated to include, where the customer is a business:

- whether, and the extent to which, the business is itself regulated under the MLRs or equivalent legislation overseas
- whether the business is, otherwise, subject to regulatory or professional conduct obligations (such as an obligation to apply CDD measures) which are effective at reducing the risk it presents
- whether the business's source of funds is regulated by a government approved scheme (e.g. as for many letting/property/estate agents in England) in a way which is relevant to the risk presented by the business relationship
- whether the business applies CDD measures to its own customers of the type required under regulation 28
- whether the purpose of the relationship or transaction presents a low risk of money laundering or terrorist financing.

1.78 These factors are drawn from guidance on SDD published by JMLSG and approved by HM Treasury. We would like to seek feedback on whether including further low risk factors in 37(3)(a), and if so which factors, could encourage greater use of SDD by regulated firms where appropriate, supported by sector-specific guidance on how they can be applied.

Pooled client accounts

1.79 The 2022 Review also found that certain types of business were struggling to access pooled client accounts (PCAs), which are a type of bank account used by brokers, agents and other businesses such as solicitors to hold client funds on behalf of a number of different clients.

1.80 While alternatives exist, PCAs are often used as a mechanism to ensure the safety of client funds in the event of firm bankruptcy, as the funds are held separately to the firm's own capital. For this reason, their use is sometimes mandated by regulatory bodies or professional associations. However, banks have lower visibility over client transactions in a PCA, compared to separate, named accounts for each individual client. While banks may be aware of the names and identities of the clients linked to a given PCA, they do not know on whose behalf a single transaction into or out of the PCA was made, because each transaction is done in the name of the firm controlling the PCA. This is an inherent limitation on the bank's ability to monitor transactions linked to a PCA for the purpose of customer due diligence.

1.81 Prior to 2017, the applicable rules were viewed as allowing banks to open PCAs without the obligation to complete due diligence on each of the clients whose money was held in the PCA, providing it was done on the firm opening the PCA. The 2017 MLRs followed updates to international standards, including those set by the FATF, to highlight the money laundering risks increasingly associated with PCAs, given their potential to obscure the source and use of funds.

1.82 The 2017 MLRs specified that simplified due diligence may be done where the business relationship or transaction presents a low degree of risk of money laundering and terrorist financing, and set specific provisions for SDD to be applied to PCAs where the customer is itself a regulated firm under the MLRs or equivalent overseas legislation. However, crucially, the MLRs are silent on whether SDD may be applied to PCAs where the customer is not a regulated firm.

1.83 To complement the risk-based approach established by the 2017 MLRs, in 2020 HM Treasury approved Joint Money Laundering Steering Group (JMLSG) guidance to help financial institutions by clarifying that they can apply SDD to low-risk, non-AML/CTF regulated businesses seeking PCAs, and specifying additional low-risk circumstances that could be considered during an individual risk assessment.

1.84 Despite the government's efforts to provide reassurance that the MLRs do not prohibit firms from applying SDD to low-risk customers, including those who are non-AML/CTF supervised, the government recognises that some businesses are still facing barriers in accessing or maintaining a client account. These include letting agents below the threshold for registering for supervision under the MLRs, yacht-brokers, care homes and certain types of business such as legal sector firms which report being unable to provide the bank with a list of clients on whose behalf monies are held in the PCA, as envisaged under regulation 37(5)(b), due to client confidentiality restrictions.

1.85 In the 2022 Review, the government concluded that broadening the circumstances in which SDD can be considered to reflect, for example, the Joint Money-Laundering Steering Group (JMLSG) guidance would be beneficial in improving access to PCAs while still ensuring that SDD can only be done in low-risk situations. The government considers that this could most effectively be done by expanding the list of low-risk customer factors in regulation 37(3)(a) as proposed above, as well as by amending 37(5) and 37(6) to clarify that PCAs may be offered to non-AML/CTF regulated customers, provided the business relationship presents a low risk of money laundering or terrorist financing.

1.86 The government recognises that applying SDD to PCAs (for instance, by not applying CDD measures directly to the individuals

on whose behalf funds are held in the PCA) carries a degree of risk for financial institutions, given the lack of visibility for the firm over individual transactions. We would like to seek views on what steps, if any, the MLRs should require firms to take to mitigate this risk.

1.87 Regulation 37(5)(b) already requires one such step, which is that information on the identity of the persons on whose behalf funds are held in the pooled client account must be available on request to the financial institution providing the account. We would like feedback on whether this requirement is effective and proportionate, and whether other mitigations might be appropriate, particularly for PCAs which are offered to AML/CTF-unregulated customers.

1.88 Other mitigations might include the following, as set out in the JMLSG guidance:

- subjecting the PCAs and/or wider business relationship to enhanced ongoing monitoring
- placing restrictions on the PCA to ensure it can only be used for the purpose for which it was established, and by the type of customers for whom it was established
- where the customer is regulated under the MLRs, agreeing a formal arrangement to rely on the due diligence measures they have already undertaken in respect of customers involved in the PCA, as envisaged by regulation 39 (Reliance on others).

1.89 In regards to the last item on relying on due diligence done by others, we recognise that this currently may only be used for one-off customer due diligence measures, and cannot therefore be used in respect of ongoing monitoring. While this is generally appropriate, in a PCA scenario there may be merit in permitting reliance to be used in respect of ongoing monitoring, given that the same transactions are involved in both relationships. We would therefore like to consult on whether we should amend regulation 39 to permit reliance in respect of ongoing monitoring in a PCA or equivalent scenario.

Q20 Do you agree that the government should expand the list of customer-related low-risk factors as suggested above?

Q21 Do you agree that as well as (or instead of) any change to the list of customer-related low-risk factors , the government should clarify that SDD can be carried out when providing pooled client accounts to non-AML/CTF regulated customers, provided the business relationship presents a low risk of money laundering or terrorist financing?

Q22 In circumstances where banks apply SDD in offering PCAs to low-risk businesses, information on the identity of the persons on whose behalf funds are held in the PCA must be made

available on request to the bank. How effective and/or proportionate do you think this risk mitigation factor is? Should this requirement be retained in the MLRs?

Q23 What other mitigations, if any, should firms consider when offering PCAs? Should these be mandatory under the MLRs?

Q24 Do you agree that we should expand the regulation on reliance on others to permit reliance in respect of ongoing monitoring for PCA and equivalent scenarios?

Q25 Are there any other changes to the MLRs we should consider to support proportionate, risk-based application of due diligence in relation to PCAs?

Chapter 2: Strengthening system coordination

Overview

2.1 AML/CTF-regulated firms and supervisory authorities are part of a wider system of public and private sector actors working together to tackle economic crime in the UK. These actors range from law enforcement agencies and other bodies dedicated wholly to combatting economic crime, to central government departments, criminal justice agencies and smaller public bodies whose role may only play an indirect part in this mission.

2.2 The effective coordination of this system is critical to its success. This is because the information, resources and capabilities needed to tackle economic crime – including money laundering and terrorist financing – are distributed across the system. No one actor can succeed without support from other actors in the system.

2.3 This chapter explores some ideas for how to strengthen system coordination via changes to the Money Laundering Regulations (MLRs). These reflect in part the need to update the MLRs, as the system evolves to take account of new and emerging threats, technological change, and changes in the legislative landscape such as the Economic Crime and Corporate Transparency Act 2023 (ECCT Act). Our proposals build on the cross-system actions set out in Economic Crime Plan 2023-26, as well as changes made when the MLRs were last amended by The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022.

2.4 Central to these ideas is the way information flows across the system. The MLRs include gateways and requirements to enable information to flow to AML/CTF supervisors and the regulated sector from other actors in the system, and vice versa. But there remains significant potential to unlock more effective dissemination of information about risks, threats and tools. The ECCT Act included measures to support this objective, including new powers for Companies House to share company data with supervisory bodies and provisions to enable sharing of information between regulated firms for the purposes of preventing, detecting and investigating economic crime. In this chapter we consider

how to build on those measures by focusing on information shared by and with the AML/CTF supervisors.

2.5 We also consider how to support the commitment in the Economic Crime Plan 2023-26 to better coordinate and prioritise our collective response to economic crime. Here, we focus on the role played by the National Risk Assessment of Money Laundering and Terrorist Financing (NRA) - the UK's stocktake of collective knowledge of the risk landscape.

Information sharing between supervisors and other public bodies

2.6 In the course of delivering their work on AML/CTF supervision, supervisors will receive a range of information from the businesses they supervise, much of it confidential or highly sensitive. This may include personal data and commercially sensitive information. For this reason, the MLRs rightly place restrictions on the circumstances in which supervisors may share information they hold in relation to their supervisory functions.

2.7 The restrictions are intended in part to ensure that regulated firms can engage openly with supervisors, with the expectation that any sensitive information disclosed will not be shared without good reason. The MLRs include specific gateways to allow for supervisors to share information with other supervisors, law enforcement agencies and other relevant public bodies for purposes related to money laundering, terrorist financing, law enforcement or the integrity of the international financial system. However, these gateways are necessarily limited in scope, and we are aware that they currently do not encompass certain legitimate forms of information sharing.

2.8 For instance, the Financial Regulators Complaints Commissioner, who is required under Part 6 of the Financial Services Act 2012 to review complaints about the actions or inactions of the UK's current financial services regulators, may sometimes be asked to investigate a complaint about the FCA's AML/CTF supervision. Neither of the information sharing gateways at regulation 52 and regulation 52A of the MLRs currently permit the sharing of information with the Financial Regulators Complaints Commissioner.

2.9 The government considers that enabling the FCA to share relevant AML/CTF-related information with the Financial Regulators Complaints Commissioner should support the effective operation of the AML/CTF system by ensuring that relevant complaints against the FCA's AML/CTF supervision can be fully investigated. However, we recognise the need to ensure that sensitive information shared by the supervisors is appropriately protected

and is not further disclosed without good reason by the recipients, for instance in the publication of reports about complaints. We would like to consult on addressing the specific issue concerning the Financial Regulators Complaints Commissioner, as well as exploring whether there are any other barriers faced by supervisors to sharing AML/CTF-related information for a legitimate purpose.

Q26 Do you agree that we should amend the MLRs to permit the FCA to share relevant information with the Financial Regulators Complaints Commissioner?

2.10 In 2022, the government made significant amendments to regulation 52 of the MLRs to expand gateways for intelligence and information-sharing, particularly between public bodies and the Professional Body Supervisors, with the aim of providing more opportunities for a whole system approach towards removing bad actors and those seeking to exploit the UK for criminal purposes.

2.11 Improving information and intelligence flows across the economic crime system is a key milestone for effective delivery of the Economic Crime Plan 2023-26, and the Office for Professional Body Anti-Money Laundering Supervisors (OPBAS) is working with Professional Body Supervisors, the National Economic Crime Centre and other partners more broadly to put in place practical arrangements to operationalise this gateway, embed these strengthened arrangements into a cross-system strategy for tackling Professional Enablers of ML and TF, and identify and address any remaining barriers to greater intelligence and information-sharing between law enforcement, supervisors, and the private sector.

2.12 Regulation 52(1A) of the MLRs provides for a reciprocal information-sharing gateway so that certain other public bodies may share AML/CTF-related information they may hold with supervisors or each other. However, the public bodies listed as relevant authorities under this provision are limited to the law enforcement agencies, HM Treasury and specific agencies under the oversight of the Department for Business and Trade.

2.13 We would like to explore whether any other public bodies should be added to this list. There may, for example, be a case for adding a body to the list if in the course of its duties it collects AML/CTF-related information which would be useful to a supervisor, and which the public body may lack powers to share under its own governing legislation.

Q27 Should we consider extending the information-sharing gateway in regulation 52(1A) to other public bodies in order to support system coordination? If so, which public bodies? Please explain your reasons.

Q28 Should we consider any further changes to the information-sharing gateways in the MLRs in order to support system coordination? Are there any remaining barriers to the effective operationalisation of regulation 52?

Cooperation with Companies House

2.14 As part of the last package of changes to the MLRs in 2022, both the Companies House Registrar and certain functions of the Secretary of State were added to the list of relevant authorities under regulation 52 for the purposes of information sharing. This means that where supervisors spot suspicious activity related to money laundering in the course of their functions, this information can be disclosed to the Companies House Registrar and other relevant authorities.

2.15 The new powers and provisions under the Economic Crime and Corporate Transparency Act 2023 will require Companies House to take a more substantive role in tackling economic crime. This includes greater powers to query and enforce the accuracy of company records on the Register. For this role to be effective, it will require cooperation with AML/CTF supervisors.

2.16 For this purpose, the government believes there may be benefit in extending the legislative basis for cooperation between Companies House and the supervisors. This might be done by expanding the relevant authorities listed under regulation 50, to include Companies House and the Secretary of State responsible for Companies House. Regulation 52 allows for information sharing to take place, regulation 50 imposes a duty on supervisors and law enforcement to cooperate with specified other authorities for the purpose of coordination, policy-making and implementation of AML/CTF financing measures. This would therefore provide more comprehensive grounds for supervisors to cooperate with Companies House, beyond just for information-sharing.

Q29 Do you agree that regulation 50 should be amended to include the Registrar for Companies House and the Secretary of State in so far as responsible for Companies House?

Q30 Do you consider there to be any unintended consequences of making this change in the way described? Please explain your reasons

Q31 In your view, what impact would this amendment have on supervisors, both in terms of costs and wider impacts? Please provide evidence where possible.

Regard for the National Risk Assessment

2.17 The UK's strengths as a global financial centre, continued openness to trade and investment and the ease of doing business here also makes us vulnerable to a wide range of economic crime. It is therefore imperative that actors within the economic crime system are aware of and understand the risks related to their sector and develop appropriate controls, policies and processes to mitigate risks and prevent abuse.

2.18 To support this objective, the MLRs 2017 stipulate that HM Treasury and Home Office must prepare a joint report setting out the findings of a risk assessment. The NRA acts as the UK's stocktake of collective knowledge of the ML and TF risks in the UK and each publication will update and build on our shared understanding of these risks. To date, we have published NRAs in 2015,[12] 2017[13] and 2020.[14]

2.19 It is also a legal requirement under the MLRs for supervisors to undertake a risk assessment and keep this assessment up to date. Supervisors are legally obliged to consider the NRA in their own risk assessments, which will identify and assess the international and domestic risks of money laundering and terrorist financing to which regulated firms in its sector are susceptible.

2.20 Under regulation 18 of the MLRs, regulated firms are required to identify the ML and TF risks to which their business may be subject to, informed by their supervisor's risk assessment and other risk factors, including their customers, jurisdictions of operation and products and services. Given this need to consult various information sources, there could be potential for a lack of clarity in the role, and extent to which, the NRA should directly inform such risk assessments.

2.21 The government is clear that taking a proportionate yet effective risk-based approach applies to all actors in the economic crime system and wants to understand if firms are sufficiently clear on the role of the NRA when meeting their obligations under the MLRs.

2.22 The government is therefore consulting on whether it should do more to clarify the relationship between the NRA and the risk assessments of regulated firms, to gather stakeholder views on

---

12 https://assets.publishing.service.gov.uk/media/5a7589a540f0b6360e474e20/UK_NRA_October_2015_final_web.pdf

13 https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017

14 https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020

this topic. The government is also interested in whether any proposed change in this area should impact supervisory activity, noting our ongoing work to reform the UK's supervisory regime.

Q32 Do you think the MLRs are sufficiently clear on how MLR-regulated firms should complete and use their own risk assessment? If not, what more could we do?

Q33 Do you think the MLRs are sufficiently clear on the sources of information MLR-regulated firms should use to inform their risk assessment (including the NRA)? If not, what more can we do?

Q34 One possible policy option is to redraft the MLRs to require regulated firms to have a direct regard for the NRA. How do you think this will impact the activity of: a) firms b) supervisors? Is there anything this obligation should or should not do?

System Prioritisation and the NRA

2.23 The Economic Crime Plan 2023-26 recognises that more can be done to coordinate and prioritise our collective response to economic crime, including a commitment to establish a set of agreed system priorities to direct collective efforts to where they will have greatest impact ('system prioritisation').

2.24 Through collaboration of the government, regulators, law enforcement, and the private sector, system prioritisation also aims to produce a single view of threats across the economic crime system, complementing and enhancing our use of intelligence to drive how threats and emerging risks are prioritised, and deprioritised, across the economic crime landscape.

2.25 While the NRA is a stock-take which takes a sectoral approach to identifying ML and TF threats in the UK, system prioritisation is intended to enable a dynamic and flexible approach to reviewing and responding to our economic crime priorities in real-time.

2.26 System prioritisation will therefore enable government and its partners to assess and evaluate threats and emerging risks at an operational and policy level across the public and private sector, deploying an increased focus and corresponding allocation of resources to the most pressing activity as appropriate.

Q35 What role do you think the NRA versus system prioritisation should play in the allocation of regulated firms' resources and design of their AML/ CTF programmes?

Chapter 3: Providing clarity on scope and registration issues

Overview

3.1 The Money Laundering Regulations (MLRs) apply to businesses which carry out certain specified activities that the government considers present a significant risk of money laundering and terrorist financing. Approximately 100,000 businesses carry out activities which fall within scope of the regulations including banks, accountants, lawyers, estate agents, casinos and other sectors.

3.2 It is important that the scope of the regulations is clear, both for businesses to understand whether they need to comply and register for AML/CTF supervision, and for supervisors to have the right tools to ensure that firms are meeting their regulatory obligations

3.3 However, the regulatory boundary which defines the scope of the MLRs (and in some cases the scope of particular requirements under the regulations) is more complex for some sectors than others. For instance, some businesses such as letting agents are subject to financial thresholds below which the regulations do not apply. Others such as lawyers, accountants, and trust and company service providers (TCSPs) are only subject to regulation in respect of certain activities. This reflects the government's risk-based approach to AML/CTF regulation, which recognises that it would be disproportionate to regulate lower-risk businesses given the burdens associated with the regulations for businesses, customers and supervisors.

3.4 This chapter considers two pressing issues with respect to the scope of the MLRs: the currency used for financial thresholds (which are currently given in a mixture of sterling and euros), and the scope of covered TCSP activity. We believe that both are in need of clarification in order to ensure the regulatory boundary remains clear and appropriately captures higher-risk business activity.

3.5 The government recognises the need for regular and more comprehensive reviews of the distribution of money laundering and terrorist financing risk across the UK economy, in order to inform the future scope of the MLRs. The appropriate vehicle for this is through updates to the National Risk Assessment of Money

Laundering and Terrorist Financing (NRA), which is jointly produced by HM Treasury and the Home Office as the UK's stocktake of collective knowledge of the ML and TF risks in the UK. To date, we have published NRAs in 2015, 2017 and 2020.

3.6 This Chapter also considers the scope of the 'fit and proper' registration regime for cryptoasset service providers, which requires clarification following the government's recent response to the consultation on the 'Future Financial Services Regulatory Regime for Cryptoassets'[15]

Currency Thresholds

3.7 Thresholds for the application of the requirements in the MLRs are currently set in a mix of currencies and contain references to both euros and pound sterling.

3.8 References to euros in the MLRs were intended to align with international FATF (Financial Action Task Force) standards which are expressed in euros and dollars, and also reflect historical transposition of EU Directives prior to the UK's exit from the European Union.

3.9 The government recognises that, following the UK's exit from the European Union, retaining a foreign currency in domestic legislation can create uncertainty and does not accurately reflect the UK's new situation.

3.10 The government is also aware that for regulated firms, such as letting agents and art market participants, with business activity around thresholds currently expressed in euros, the need to regularly convert from sterling to euros as exchange rates fluctuate can pose an administrative burden. It can also lead to potential confusion about whether businesses are within scope of the MLRs or not, depending on the exchange rate.

3.11 The government remains committed to easing the administrative burdens for firms to comply with the regulations and addressing the need for consistency while complying with international FATF standards, and also reflecting the UK's new status as a non-EU member state.

3.12 The FATF standards currently state that financial institutions and dealers in precious metals and stones should be required to undertake customer due diligence (CDD) measures when carrying out occasional transactions above the applicable designated threshold (USD/EUR 15,000), and casinos when their customers

15 https://www.gov.uk/government/consultations/future-financial-services-regulatory-regime-for-cryptoassets

engage in financial transactions equal to or above USD/EUR 3,000. However, the threshold for customer due diligence in the UK's MLRs are set below this at 10,000 euros for high value dealers, estate agent businesses, letting agents and art market participants, and set at the limit of 15,000 euros for relevant persons who are not high value dealers.

3.13 Following the UK's exit from the European Union, and given that the UK is not a member of the Euro, the government's preferred option is that thresholds in the MLRs are expressed in pound sterling.

3.14 In light of this, the government is therefore consulting to ascertain the scale and significance of any administrative burdens currently faced by firms by the inclusion of euros in the MLR thresholds, and to understand the potential impact of any future shift in the regulations to the exclusive use of pound sterling.

Q36 In your view, are there any reasons why the government should retain references to euros in the MLRs?

Q37 To what extent does the inclusion of euros in the MLRs cause you/your firm administrative burdens? Please be specific and provide evidence of the scale where possible.

Q38 How can the UK best comply with threshold requirements set by the FATF?

3.15 The government remains committed to maintaining regulatory compliance with international standards outlined in the FATF Recommendations and is not considering significant changes in the values of the thresholds at this time. There are, however, different ways in which the government could achieve a currency change without significantly altering the value of the thresholds themselves:

3.16 **Option A: Change all references to euros into pounds on a 1:1 basis.** Under this option a threshold of 10,000 euros would become £10,000 sterling. This would represent a slight raise in the threshold. This would be the simplest option but would run the risk of the UK not complying with the FATF standards in certain areas of the MLRs. This would be the case where existing thresholds are already set at the FATF maximum, such as in regulation 27(2) for occasional transactions. A slight raise to this threshold resulting from a 1:1 conversion could therefore place the UK threshold above what the FATF recommends. Additionally, it could also lead to misalignment in the future if exchange rates fluctuate, and as a result would have to be kept under review.

3.17 **Option B:** Convert **all references to euros into pounds using an average exchange rate and round down.** For instance, under this option a threshold of 10,000 euros might be converted to c. £8,666 and rounded down to £8,000 sterling for administrative ease. This

would represent a slight lowering of the threshold but would help guard against fluctuations in exchange rates that might cause misalignment with the FATF standards and so minimise the need for future changes to ensure alignment.

Q39 If the government were to change all references to euros in the MLRs to pound sterling which of the above conversion methods (Option A or Option B) do you think would be best course of action?

Q40 Please explain your choice and outline with evidence, where possible, any expected impact that either option would have on the scope of regulated activity.

Regulation of resale of companies and off the shelf companies by TCSPs

3.18 A trust and company service provider (TCSP) is a business or individual that provides services, as defined in the MLRs, related to the incorporation, management, or administration of legal entities such as trusts or companies.

3.19 TCSPs as part of their suite of services will often set up and administer onward sale of 'off the shelf' companies. These are limited companies already registered in the UK at Companies House, but that are dormant or non-trading. They have not usually been set up for a specific buyer meaning address or director details will often be changed on sale. Unlike TCSP services defined under the MLRs the onward sale of such companies is not currently regulated.

3.20 The scope to enhance anonymity can make corporate structures an attractive tool for criminals, and their use is regularly identified within money laundering investigations. Whilst the vast majority of UK companies are used for legitimate purposes, as the UK is a global financial centre there is a high risk that economic crime in the UK will involve the abuse of a corporate vehicle. The government has taken significant action to address this, passing the Economic Crime and Corporate Transparency Act in 2023 to give Companies House new powers to crack down on the misuse of UK companies. Ensuring that TCSPs are not misused is also vital to the government's efforts to preserve the integrity of the UK economy. The government intends to support these objectives by addressing any remaining gaps in the TCSP regime.

3.21 The government believes now is the right time to consult on extending TCSP activity to include the sale of off the shelf companies. This has been a longstanding gap in the current AML/CTF regime with evidence of abuse.

3.22 TCSP activity as defined under Regulation 12(2) of the MLRs includes where the TCSP 'forms a firm' as a service for third parties. However, the MLRs do not specifically cover where the formation of a firm is not for a specific customer but is intended to be held in stock. The MLRs also do not cover the onward sale of these firms. The government recognises that the speed with which TCSP-formed firms can be deployed is an important tool for competitiveness within the UK commercial services space. However, there is evidence to suggest that the lack of due diligence checks on purchase of these 'off-the-shelf' companies means that they are at risk of being used for illicit purposes. In particular, off-the-shelf companies may be deliberately 'matured' for a number of years before sale. This will lend a sense of legitimacy to the companies so is appealing to bad faith actors. Therefore, the government is seeking views on amending the wording of regulation 12(2)(a) to include the sale of firms within the scope of regulated TCSP activity. This will ensure TCSPs are required to apply the regulations as appropriate when carrying out the sale of a firm that they have set up or bought for later onward sale, including to apply customer due diligence measures.

Q41 Do you agree that regulation 12(2) (a) and (b) should be extended to include formation of firms without an express request, sale to a customer or a person acting on the customer's behalf and acquisition of firms to sell to a customer or a person acting on the customer's behalf?

Q42 Do you consider there to be any unintended consequences of making this change in the way described? Please explain your reasons.

Q43 In your view, what impact would this amendment have on TCSPs, both in terms of costs and wider impacts? Please provide evidence where possible.

Change in control for cryptoasset service providers

Regulation for registration and change in control of custodial wallet providers and cryptoasset exchange providers

3.23 A range of credit and financial institutions supervised by the Financial Conduct Authority (FCA) under the Money Laundering Terrorist Financing and Transfer of Funds Regulations 2017 are also authorised by the FCA in its capacity as a regulator under the Financial Services and Markets Act 2000 (FSMA). 'Authorised' under FSMA means that the institution or person has met the standards required by FSMA and can comply with the relevant

principles and rules in the FCA Handbook. To avoid duplication, FSMA authorised institutions or persons that are also subject to the MLRs are not required to seek authorisation for the equivalent financial services activity separately with the FCA for MLR purposes.

3.24 The MLRs were extended in 2019[16] to include 'cryptoasset exchange providers' and 'custodian wallet providers' ["crypto firms"]. This was in response to a 2018 update to the international standards on money laundering and counter terrorist financing set by the Financial Action Taskforce (FATF). The FCA was made the supervisory authority responsible for AML/CTF supervision of crypto firms.

3.25 Most crypto firms supervised by the FCA are not FSMA authorised, so the MLRs contain a bespoke registration process for them. Currently, this applies to all crypto firms, including the minority of crypto firms that are also FSMA authorised, meaning that if a firm wishes to undertake cryptoasset activity and is already FSMA authorised, they have to register separately under the MLRs. To become registered, a crypto firm and any officer, manager, or beneficial owner of the firm must, amongst other procedures, pass an FCA fit and proper assessment.

3.26 In 2022 the MLRs were further amended to include change in control provisions. This requires certain persons to notify the FCA that they intend to acquire control over an MLR registered crypto firm by becoming a 'beneficial owner'. The FCA is then required to carry out a fit and proper assessment on that person. The FCA can then either approve the acquisition, approve with conditions or object.

3.27 On the 30th of October 2023 the government released a response[17] to its 'Future Financial Services Regulatory Regime for Cryptoassets' consultation. The response includes how specific activities related to cryptoassets could be brought under the broader FSMA regime, bringing them in line with the wider financial sector[18].

3.28 The proposed change will capture many crypto firms currently registered with the FCA for MLR purposes only. It is the

---

16 https://www.legislation.gov.uk/uksi/2019/1511/contents/made

17 https://assets.publishing.service.gov.uk/media/653bd1a180884d0013f71cca/Future_financial_services_regulatory_regime_for_cryptoassets_RESPONSE.pdf

18 https://assets.publishing.service.gov.uk/media/653bd1a180884d0013f71cca/Future_financial_services_regulatory_regime_for_cryptoassets_RESPONSE.pdf, p22

government's intention that these MLR only registered crypto firms will need to apply for FSMA authorisation when the new regime comes into force, but authorisation under both the MLRs and FSMA will no longer be required. This should similarly apply to firms currently FSMA authorised for wider financial services who intend to add cryptoasset services into their business model. This issue was raised in response to the government's consultation on the Digital Securities Sandbox (DSS) in 2023. Activity in the DSS, including the issuance, trading, settlement and maintenance of security tokens may be caught within the scope of regulation 14a of the MLRs. Applicants for the DSS will be FSMA authorised firms who are unlikely to be MLRs registered for cryptoasset activities. Under the current system DSS applications would still have to register under the MLRs separately. HMT will work with the regulators to determine how the application of the MLRs to DSS activity should be addressed.

Firms within scope of the MLRs

3.29 As noted in the 2023 consultation response[19], the scope of crypto firms subject to the new FSMA regime will be narrower than those subject to the MLRs.

3.30 The definition of 'cryptoasset exchange providers' and 'custodian wallet providers' in the MLRs captures a broad range of activities involving cryptoassets. This is coupled with a broad definition of cryptoassets as "a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically". For cryptoasset exchange activity, the definition is extended further to include a right to, or interest in, a cryptoasset. This definition effectively covers any digital token which represents some kind of value, ownership of which is recorded on a blockchain.

3.31 Some cryptoassets are caught by existing FSMA regulation, for example if they serve as the underlying asset or property for regulated activities or financial instruments, such as in collective investment schemes. The new FSMA regime for cryptoassets will bring in a number of new regulated activities such as operating a cryptoasset exchange and custody. However, some cryptoassets will not be used in relation to any financial services regulated activity criteria and potentially fall outside the regime. This means

19 https://assets.publishing.service.gov.uk/media/653bd1a180884d0013f71cca/Future_financial_services_regulatory_regime_for_cryptoassets_RESPONSE.pdf, p19 and p32

that the MLRs may capture cryptoasset activities and the firms undertaking them that are not within the FSMA regime. These cryptoasset firms will still need to be registered and supervised by the FCA for anti-money laundering and counter terrorist financing purposes.

3.32 Cryptoasset firms that the government believes may fall into this category are likely to be those who issue or provide services for cryptoassets that are not financial in nature; for example, firms that provide certain types of non-fungible or experience tokens[20] where they are not used as part of a regulated activity. The number and types of firms in this category may widen as the industry continues to develop. The government recognises such tokens and associated services can still present ML/TF risks.

Issue

3.33 The authorisation/registration and change in control assessments under FSMA and the MLRs differ in how they identify and assess the risks associated with controllers of crypto firms. This is because FSMA and the MLRs identify control and controllers of crypto firms based on different definitions. In particular, the type of people who can have control and the thresholds for that control are different between the regimes.

3.34 A comparison between the MLRs provisions and the FSMA provisions for authorisation/registration and change in control is set out in the table below-

	MLRs	**FSMA**
Persons capable of having control/those required to give notice of control	Natural persons (with minor exceptions for trusts).	Any person, whether legal or natural.
Definition of control/controllers	A 'beneficial owner' The definition of 'beneficial owner' depends on the type of entity. Most crypto firms are body corporates that are not listed on a	A 'controller' This is a person who holds 10% or more of the shares or voting power in the crypto firm or a

[20] https://assets.publishing.service.gov.uk/media/653bd1a180884d0013f71cca/Future_financial_services_regulatory_regime_for_cryptoassets_RESPONSE.pdf, p32

	regulated market, and in this context a 'beneficial owner' generally means an individual who ultimately owns or controls more than 25% of shares or voting power in the relevant crypto firm.	parent undertaking of the firm. Each parent undertaking in the chain will be a controller and the definition of 'voting power' extends to include voting power held by a controlled undertaking.
Thresholds for when notice is required under change in control regime	When an individual decides to become a beneficial owner. Existing beneficial owners do not need to notify of an increase to their control.	When a person decides to acquire control by becoming a controller (see above). When a controller decides to increase their control and passes through control thresholds of 20%, 30% and 50%. Note: These thresholds have been modified for some FSMA authorised persons by the Financial Services and Markets Act 2000 (Controllers) (Exemption) Order 2009.
Other persons caught by change in control assessment	Only considers the beneficial owner.	Will include an assessment of the reputation, knowledge, skills and experience of any person who will direct the business of the crypto firm as a result of the proposed acquisition.

3.35 The government is interested in views as to whether it is appropriate to have two different concepts of control for crypto

firms under MLR supervision depending on whether they are FSMA authorised or not.

3.36 Subject to analysis of responses to this consultation, the government proposes to align the current MLR regime for crypto firms more closely with the FSMA model. This would mean changing the type of persons who are subject to assessment under the fit and proper test and the thresholds for assessment to capture those who are actually exercising control over crypto firms. Firms under each regime in the same industry should as a matter of principle have commensurate risk of money laundering and terrorist financing and consequently be treated the same in regulation. Our intention is that this should have the added benefit of making it easier for currently authorised crypto firms to move into the FSMA regime, as they will have already identified relevant controllers under the MLRs.

Q44 Do you agree that the MLRs should be updated to take into account the upcoming regulatory changes under FSMA regime? If not, please explain your reasons.

Q45 Do you have views on the sequencing of any such changes to the MLRs in relation to the upcoming regulatory changes under the FSMA regime? If yes, please explain.

Q46 Do you agree that this should be delivered by aligning the MLRs registration and FSMA authorisation process, including the concepts of control and controllers, for cryptoassets and associated services that are covered by both the MLRs and FSMA regimes? If not, please explain your reasons.

Q47 In your view, are there unique features of the cryptoasset sector that would lead to concerns about aligning the MLRs more closely with a FSMA style fit and proper process? If yes, please explain.

Q48 Do you consider there to be any unintended consequences to closer alignment in the way described? If yes, please explain.

Chapter 4: Reforming registration requirements for the Trust Registration Service

Overview

The Trust Registration Service

4.1 A trust is a way of managing assets such as land, buildings and money. It involves the splitting of asset ownership into 'legal' and 'beneficial' ownership: the trustees are the legal owners, and holders of the trust assets which they manage for the other beneficial owners. For the Trust Registration Service (TRS) "Beneficial Owners" are defined as generally anyone with a legal interest in the trust such as the settlor, the trustees or the beneficiaries and may be individuals, corporate entities or other organisations such as charities.

4.2 There are a wide range of reasons trusts are used in the UK, including protecting assets for a vulnerable individual or bringing together investments for grandchildren. However, because trusts are arranged privately, they can also be used to conceal the beneficial ownership of assets, and thereby facilitate money laundering and terrorist financing.

4.3 The TRS was introduced in 2017 by the Money Laundering Regulations (MLRs), to increase the transparency of trust ownership by providing a central register of the beneficial ownership of taxable trusts. Changes to the MLRs since then mean that the TRS now is a register of most types of UK express trusts and some non-UK express trusts.[21]

[21] There are many different kinds of trust. Trust arrangements may be expressly created by a settlor, often in a formal legal document, known as an 'express trust', but this is not always the case; trusts that are not expressly created by a settlor are known as 'implied trusts'. Details on which trusts are required to register can be found here: https://www.gov.uk/guidance/register-a-trust-as-a-trustee

4.4 The purpose of the TRS is to document information about trusts and to make it available to law enforcement agencies to assist with their investigations. Since 1 September 2022, individuals and organisations can also access TRS information in certain limited circumstances. All individuals and organisations can access trust data where a trust has a controlling interest in an 'offshore company'. Access to all other trust data requires the requester to have a "legitimate interest" in that trust information. A legitimate interest is demonstrated through evidence including an individual or organisation being involved in an investigation into money laundering and terrorist financing.

4.5 HMRC has overall responsibility for the TRS. Trustees have a responsibility to register their trusts, if they fall within the registration rules, and to keep the trust information up to date. Trustees of registrable trusts must also provide proof of registration to certain 'relevant persons', as set out in the MLRs. Relevant persons are advised not to do business with registerable trusts that fail to show proof of registration and must report to HMRC any material discrepancies between the information they hold on the trust and the information held on TRS.

Reviewing the Trust Registration Service

4.6 The government is reviewing the operation and scope of the TRS: the role of TRS in the investigation of money laundering and terrorist financing; the registration responsibility on trustees; and the changing international and national objectives to increase transparency of trusts. The purpose of the review is to identify areas where the TRS could be improved to continue meeting key policy objectives and to provide consistency and simplicity.

4.7 The government wants a targeted approach to trust registration requirements, to focus the requirements on the highest risk trusts. The government proposes to make changes to the TRS to include:

- requiring the registration of all non-UK express trusts with no UK trustees, that own UK land
- sharing trust information of non-UK express trusts with no UK trustees that own UK land by making these trusts subject to the current Trust Data Sharing process[22]
- aligning the registration requirements of some trusts required to register following the death of a settlor

[22] https://www.gov.uk/hmrc-internal-manuals/trust-registration-service-manual/trsm60020

- clarifying that Scottish survivorship destination trusts are not required to register
- introducing a de minimis level for trust registration.

Registration of non-UK express trusts with no UK trustees, that own UK land

4.8 The government is also consulting on the wider issues of the transparency of ownership of UK land.[23] The National Risk Assessment (NRA) for Money Laundering and Terrorist Financing 2020 observed that the property sector faces a high risk from money laundering, due to the large amounts of cash that can be moved / invested in the sector and that non-UK trusts "...are likely to be more attractive for illicit purposes as they can offer better levels of secrecy and tax advantages compared to UK-based trusts".

4.9 It is against this backdrop that the government seeks to improve the transparency of UK land ownership by non-UK trusts through increasing the scope of trusts that are required to be registered on the TRS.

Registration of non-UK express trusts, with no UK trustees, that acquired UK land before 6 October 2020

4.10 Since 6 October 2020, the MLRs have required non-UK express trusts, with no UK trustees, to register on the TRS if the trustees acquire land in the UK.

4.11 This means such trusts that acquired UK land or property before 6 October 2020 are not currently registered on the TRS.

4.12 The Register of Overseas Entities (ROE is operated by Companies House and collects information about registrable overseas entities (mainly non-UK companies) that own land or property in the UK. Some of these entities are corporate trustees.

4.13 Where trustees beneficially own overseas entities – the beneficial ownership details (settlors, beneficiaries etc) are recorded on ROE. However, where a corporate trustee owns land directly, the ROE only captures the corporate trustee's details.

4.14 For example, a corporate entity acting as a trustee for multiple trusts could own many UK properties directly but the ROE captures no information about the beneficial owners of that land:

---

[23] https://www.gov.uk/government/consultations/transparency-of-land-ownership-involving-trusts-consultation/transparency-of-land-ownership-involving-trusts#:~:text=This%20consultation%20aims%20to%20lift,sensitively%2C%20with%20the%20right%20safeguards.

only the details of the corporate trustee. Additionally, different implementation dates for registration of overseas entities in the individual UK countries means that registration is not consistent across the UK.

4.15 The government recognises that there is currently a reporting gap of direct UK land ownership by wholly non-UK trusts. The government therefore proposes to extend the requirement to register on TRS to include trusts that acquired UK land before 6 October 2020.

Trust data requests: non-UK express trusts, with no UK trustees, that own UK land

4.16 Since September 2022, individuals or organisations can request information held on the TRS in certain circumstances using the Trust Data Request process.[24] There are two types of Trust Data Requests:

- legitimate interest - the requester is making a request because they can show they are involved in an investigation of money laundering or terrorist financing and are requesting access to further this investigation
- offshore company - the requester is making a request because the trustees of the trust subject to their request have a controlling interest in an offshore company.

4.17 Currently a Trust Data Request cannot be made to access information held on non-UK express trusts, with no UK trustees, that have acquired UK land. In other words, this information cannot be shared with persons outside of law enforcement agencies. The government has been criticised by transparency organisations arguing lack of access to data on these trusts could undermine its objective to bring greater transparency of the ownership of UK land by entities outside the UK.

4.18 The government is proposing to extend the TRS trust data sharing rules to include these trusts.

Q49 Does the proposal to make these trusts that acquired UK land before 6 October 2020 register on TRS cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.

---

[24] For detail on the Trust Data Request process please see TRSM60000 HMRC Internal Manual – Trust Registration Service Manual: https://www.gov.uk/hmrc-internal-manuals/trust-registration-service-manual/trsm60000

Q50 Does the proposal to change the TRS data sharing rules to include these trusts cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.

Trusts required to register following a death

4.19 Wills commonly create a trust upon someone's death. In many of these cases, once the estate has finished being administered by the executors, the trust ceases to exist. These trusts would typically present a low risk for facilitating money laundering and terrorist financing. Currently these 'will trusts' are excluded from registering on TRS for a period of two years from the date of death.

4.20 However, there are other types of trust that become registrable on the death of an individual with different deadlines for registration on the TRS. Some of these are existing trusts which were not required to register on TRS when the person was alive and some are trusts created as part of the estate administration process, namely:

- co-ownership property trusts currently must be registered on TRS within 90 days of a person's death
- trusts created by deed of variation currently must be registered on TRS within 90 days of being created.

4.21 The government believes that a common registration deadline for those trusts associated with the estate of a deceased person will enable better compliance with the registration requirements.

Trusts required to register following a death: Co-ownership Property Trusts

4.22 Co-ownership trusts are trusts of jointly held property where the trustees and beneficiaries are the same persons and are excluded from registration. These trusts often arise in the purchasing of land and property in England and Wales.

4.23 Co-ownership property trusts are currently excluded from registration. However, upon the death of one of the parties, as the trustees are no longer the same as the beneficiaries, the trust becomes registrable.

4.24 The government is proposing to exclude co-ownership property trusts that would become registrable upon death from registration for two years from the date of death. This will align the timing of registration with will trusts that become registrable on death.

Trusts required to register following a death: trusts created by deed of variation

4.25 Deeds of variation are typically a method of redistributing the property of a deceased person's estate. They are used when the beneficiaries agree to redistribute the estate, for instance if one of the parties decide not to inherit the property.

4.26 Trusts created by deeds of variation are express trusts and therefore registrable within 90 days of being created.

4.27 The government is proposing to exclude all trusts created by deed of variation that would become registrable upon death from registration, for two years from the date of death. This will align the timing of registration with will trusts that become registrable on death.

Q51 Do the proposals to exclude these trusts for two years from the date of death cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.

Scottish survivorship destination trusts

4.28 In Scotland it is possible for property to be owned jointly by property owners where the title to the property contains a special destination, known as a survivorship clause or survivorship destination. This clause directs that the property is held equally for the owners and the survivor. To revoke the survivorship destination after the property has been registered in the Land Register of Scotland, the property owners may either register a new deed in the land register where they will incur registration fees or create a trust that records that the survivorship destination has been revoked and sets out the new beneficiary of the property.

4.29 Where a trust is created to revoke a special destination, this is an express trust, and it is therefore currently registrable on TRS. Under English and Welsh Law, achieving this outcome would not result in a registrable trust. The government believes that such trusts present a low risk of facilitating money laundering and terrorist financing.

4.30 The government is proposing to exclude Scottish survivorship destination trusts from TRS registration.

Q52 Does the proposal to exclude Scottish survivorship destination trusts cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.

De minimis exemption for registration

4.31 The NRA 2020 noted that offshore activity, property and cash transactions were indicative of high risk in terms of money laundering and terrorist financing. The government considers that a risk-based approach to the registration of trusts is the appropriate mechanism for achieving the objectives of the MLRs and that under specific circumstances, small, low value trusts could be made exempt from registration.

4.32 To this end, the government proposes to introduce a de minimis exemption for trusts required to register on the TRS. The de minimis exemption seeks to differentiate between small low value trusts and the higher risk trusts that hold property.

4.33 Responsibility to determine whether a trust qualifies as being de minimis would fall to the trustees.

4.34 The government is proposing to exclude from registration a trust that meets all of the following tests:

- the trust is not liable for relevant UK taxes
- the trust does not own or have an interest, in whole or in part, in UK land/real property
- the trust does not hold more than £5,000 in assets
- the trust does not distribute more than £2,000 in assets and expenses (combined) in any 12-month period.

4.35 Once a trust exceeds any of the threshold amounts, the trust would become registerable and remain registerable. For instance, were the value of a trust's assets to be above £5,000 and then fall below this amount, then the trust would remain registerable.

4.36 From tax year 2024-25 a new tax rule will take trusts out of income tax where their income is less than £500, allowing more trusts to meet the first test.

4.37 The government similarly recognises that some settlors may attempt to create multiple trusts in order to meet the proposed de minimis criteria for registration above. To this end the government proposes to put restrictions in place to prevent this from happening.

Q53 Does the proposal to create a de minimis level for registration cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.

Q54 Do you have any views on the proposed de minimis criteria?

Q55 Do you have any proposals regarding what controls could be put in place to ensure that there is no opportunity to use the de minimis exemption to evade registration on TRS?

Annex A: HM Treasury consultations – processing of personal data

Processing of personal data

This section sets out how we will use your personal data and explains your relevant rights under the UK General Data Protection Regulation (UK GDPR). For the purposes of the UK GDPR, HM Treasury is the data controller for any personal data you provide in response to this consultation.

Data subjects

The personal data we will collect relates to individuals responding to this consultation. These responses will come from a wide group of stakeholders with knowledge of a particular issue.

The personal data we collect

The personal data will be collected through email submissions and are likely to include respondents' names, email addresses, their job titles and opinions.

How we will use the personal data

This personal data will only be processed for the purpose of obtaining opinions about government policies, proposals, or an issue of public interest.

Processing of this personal data is necessary to help us understand who has responded to this consultation and, in some cases, contact certain respondents to discuss their response.

HM Treasury will not include any personal data when publishing its response to this consultation.

Lawful basis for processing the personal data

Article 6(1)(e) of the UK GDPR; the processing is necessary for the performance of a task we are carrying out in the public interest. This task is consulting on the development of departmental policies or proposals to help us to develop effective government policies.

Who will have access to the personal data

The personal data will only be made available to those with a legitimate need to see it as part of consultation process.

We will share responses to the questions in Chapter 4 with HMRC because of their responsibility of the Trust Registration Service. This will include the names of respondents only, any other directly identifiable personal data will not be shared.

We may also share anonymised extracts from responses with other government departments, law enforcement agencies and AML supervisors, in order to discuss particular issues or help develop policies.

As the personal data is stored on our IT infrastructure, it will be accessible to our IT service providers. They will only process this personal data for our purposes and in fulfilment with the contractual obligations they have with us.

How long we hold the personal data for

We will retain the personal data until work on the consultation is complete and no longer needed.

Your data protection rights

Relevant rights, in relation to this activity are to:

- request information about how we process your personal data and request a copy of it
- object to the processing of your personal data
- request that any inaccuracies in your personal data are rectified without delay
- request that your personal data are erased if there is no longer a justification for them to be processed
- complain to the Information Commissioner's Office if you are unhappy with the way in which we have processed your personal data

How to submit a data subject access request (DSAR)

To request access to your personal data that HM Treasury holds, please email: dsar@hmtreasury.gov.uk

Complaints

If you have concerns about Treasury's use of your personal data, please contact our Data Protection Officer (DPO) in the first instance at: privacy@hmtreasury.gov.uk

If we are unable to address your concerns to your satisfaction, you can make a complaint to the Information Commissioner at casework@ico.org.uk or via this website: https://ico.org.uk/make-a-complaint.

Annex B: Question list

Chapter 1: Making customer due diligence more proportionate and effective

Customer Due Diligence

Due diligence triggers for non-financial firms

Q1 **Are the customer due diligence triggers in regulation 27 sufficiently clear?**

Source of funds checks

Q2 **In your view, is additional guidance or detail needed to help firms understand when to carry out 'source of funds' checks under regulation 28(11)(a)? If so, in what form would this guidance be most helpful?**

Verifying whether someone is acting on behalf of a customer

Q3 **Do you think the wording in regulation 28(10) on necessary due diligence on persons acting on behalf of a customer is sufficiently clear? If not, what could help provide further clarity?**

Digital identity verification

Q4 **What information would you like to see included in published digital identity guidance, focused on the use of digital identities in meeting MLR requirements? Please include reference to the level of detail, sources or types of information to support your answer.**

Q5 **Do you currently accept digital identity when carrying out identity checks? Do you think comprehensive guidance will provide you with the confidence to accept digital identity, either more frequently, or at all?**

Q6 **Do you think the government should go further than issuing guidance on this issue? If so, what should we do?**

Timing of verification of customer identity

Q7 **Do you think a legislative approach is necessary to address the timing of verification of customer identity following a bank insolvency, or would a non-legislative approach be sufficient to clarify expectations?**

Q8 **Are there other scenarios apart from bank insolvency in which we should consider limited carve-outs from the requirement**

to ensure that no transactions are carried out by or on behalf of new customers before verification of identity is complete?

Enhanced Due Diligence

General triggers for enhanced due diligence

Q9 **(If relevant to you) Have you ever identified suspicious activity through enhanced due diligence checks, as a result of the risk factors listed above? (Regulations 33(6)(a)(vii), 33(6)(a)(viii) and 33(6)(b)(vii)). Can you share any anonymised examples of this?**

Q10 **Do you think that any of the risk factors listed above should be retained in the MLRs?**

Q11 **Are there any risk factors for enhanced due diligence, set out in regulation 33 of the MLRs, which you consider to be not useful at identifying suspicious behaviour?**

Q12 **In your view, are there any additional risk factors that could usefully be added to, for example, regulation 33, which might help firms identify suspicious activity?**

'Complex or unusually large' transactions

Q13 **In your view, are there occasions where the requirement to apply enhanced due diligence to 'complex or usually large' transactions results in enhanced due diligence being applied to a transaction which the relevant person is confident to be low-risk before carrying out the enhanced checks? Please provide any anonymised examples of this and indicate whether this is a common occurrence.**

Q14 **In your view, would additional guidance support understanding around the types of transactions that this provision applies to and how the risk-based approach should be used when carrying out enhanced check?**

Q15 **If regulation 33(1)(f) was amended from 'complex' to 'unusually complex' (e.g. a relevant person must apply enhanced due diligence where… 'a transaction is unusually complex or unusually large'):**

- **in your view, would this provide clarity of intent and reduce concern about this provision? Please explain your response.**
- **in your view, would this create any problems or negative impacts?**

High Risk Third Countries

Q16 **Would removing the list of checks at regulation 33(3A), or making the list non-mandatory, reduce the current burdens (cost and time etc.) currently placed on regulated firms by the HRTC rules? How?**

Q17 **Can you see any issues or problems arising from the removal of regulation 33(3A) or making this list non-mandatory?**

Q18 **Are there any High Risk Third Country-established customers or transactions where you think the current requirement to carry out EDD is not proportionate to the risk they present? Please provide examples of these and indicate, where you can, whether this represents a significant proportion of customers/transactions.**

Q19 **If you answered yes to the above question, what changes, if any, could enable firms to take a more proportionate approach? What impact would this have?**

Simplified Due Diligence

Pooled client accounts

Q20 **Do you agree that the government should expand the list of customer-related low-risk factors as suggested above?**

Q21 **Do you agree that as well as (or instead of) any change to the list of customer-related low-risk factors , the government should clarify that SDD can be carried out when providing pooled client accounts to non-AML/CTF regulated customers, provided the business relationship presents a low risk of money laundering or terrorist financing?**

Q22 **In circumstances where banks apply SDD in offering PCAs to low-risk businesses, information on the identity of the persons on whose behalf funds are held in the PCA must be made available on request to the bank. How effective and/or proportionate do you think this risk mitigation factor is? Should this requirement be retained in the MLRs?**

Q23 **What other mitigations, if any, should firms consider when offering PCAs? Should these be mandatory under the MLRs?**

Q24 **Do you agree that we should expand the regulation on reliance on others to permit reliance in respect of ongoing monitoring for PCA and equivalent scenarios?**

Q25 **Are there any other changes to the MLRs we should consider to support proportionate, risk-based application of due diligence in relation to PCAs?**

Chapter 2: Strengthening system coordination

Information sharing between supervisors and other public bodies

Q26 **Do you agree that we should amend the MLRs to permit the FCA to share relevant information with the Financial Regulators Complaints Commissioner?**

Q27 **Should we consider extending the information-sharing gateway in regulation 52(1A) to other public bodies in order to support system coordination? If so, which public bodies? Please explain your reasons.**

Q28 **Should we consider any further changes to the information-sharing gateways in the MLRs in order to support system coordination? Are there any remaining barriers to the effective operationalisation of regulation 52?**

Cooperation with Companies House

Q29 **Do you agree that regulation 50 should be amended to include the Registrar for Companies House and the Secretary of State in so far as responsible for Companies House?**

Q30 **Do you consider there to be any unintended consequences of making this change in the way described? Please explain your reasons**

Q31 **In your view, what impact would this amendment have on supervisors, both in terms of costs and wider impacts? Please provide evidence where possible.**

Regard for the National Risk Assessment

Q32 **Do you think the MLRs are sufficiently clear on how MLR-regulated firms should complete and use their own risk assessment? If not, what more could we do?**

Q33 **Do you think the MLRs are sufficiently clear on the sources of information MLR-regulated firms should use to inform their risk assessment (including the NRA)? If not, what more can we do?**

Q34 **One possible policy option is to redraft the MLRs to require regulated firms to have a direct regard for the NRA. How do you think this will impact the activity of: a) firms b) supervisors? Is there anything this obligation should or should not do?**

System Prioritisation and the NRA

Q35 What role do you think the NRA versus system prioritisation should play in the allocation of regulated firms' resources and design of their AML/ CTF programmes?

Chapter 3: Providing clarity on scope and registration issues

Currency Thresholds

Q36 In your view, are there any reasons why the government should retain references to euros in the MLRs?

Q37 To what extent does the inclusion of euros in the MLRs cause you/your firm administrative burdens? Please be specific and provide evidence of the scale where possible.

Q38 How can the UK best comply with threshold requirements set by the FATF?

Q39 If the government were to change all references to euros in the MLRs to pound sterling which of the above conversion methods (Option A or Option B) do you think would be best course of action?

Q40 Please explain your choice and outline with evidence, where possible, any expected impact that either option would have on the scope of regulated activity.

Regulation of resale of companies and off the shelf companies by TCSPs

Q41 Do you agree that regulation 12(2) (a) and (b) should be extended to include formation of firms without an express request, sale to a customer or a person acting on the customer's behalf and acquisition of firms to sell to a customer or a person acting on the customer's behalf?

Q42 Do you consider there to be any unintended consequences of making this change in the way described? Please explain your reasons.

Q43 In your view, what impact would this amendment have on TCSPs, both in terms of costs and wider impacts? Please provide evidence where possible.

Change in control for cryptoasset service providers

Q44 **Do you agree that the MLRs should be updated to take into account the upcoming regulatory changes under FSMA regime? If not, please explain your reasons.**

Q45 **Do you have views on the sequencing of any such changes to the MLRs in relation to the upcoming regulatory changes under the FSMA regime? If yes, please explain.**

Q46 **Do you agree that this should be delivered by aligning the MLRs registration and FSMA authorisation process, including the concepts of control and controllers, for cryptoassets and associated services that are covered by both the MLRs and FSMA regimes? If not, please explain your reasons.**

Q47 **In your view, are there unique features of the cryptoasset sector that would lead to concerns about aligning the MLRs more closely with a FSMA style fit and proper process? If yes, please explain.**

Q48 **Do you consider there to be any unintended consequences to closer alignment in the way described? If yes, please explain.**

Chapter 4: Reforming registration requirements for the Trust Registration Service

Registration of non-UK express trusts with no UK trustees, that own UK land

Q49 **Does the proposal to make these trusts that acquired UK land before 6 October 2020 register on TRS cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.**

Q50 **Does the proposal to change the TRS data sharing rules to include these trusts cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.**

Trusts required to register following a death

Q51 **Do the proposals to exclude these trusts for two years from the date of death cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.**

Q52 **Does the proposal to exclude Scottish survivorship destination trusts cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.**

De minimis exemption for registration

Q53 Does the proposal to create a de minimis level for registration cause any unintended consequences? If so, please describe these, and suggest an alternative approach and reasons for it.

Q54 Do you have any views on the proposed de minimis criteria?

Q55 Do you have any proposals regarding what controls could be put in place to ensure that there is no opportunity to use the de minimis exemption to evade registration on TRS?

Annex C: Glossary

2022 Review – HM Treasury's 2022 review of the UK's AML/CTF regime

AML/CTF - Anti-Money Laundering and Counter Terrorism Financing

CDD – Customer Due Diligence

Crypto firms - Cryptoasset exchange providers and 'custodian wallet providers

DPDI Bill – Data Protection and Digital Information Bill

ECCTA/ECCT Act - Economic Crime and Corporate Transparency Act

ECP2 – Economic Crime Plan 2

EDD – Enhanced Due Diligence

EU – European Union

FATF – Financial Action Task Force

FATF Standards: The FATF Recommendations (a comprehensive framework of measures to help countries tackle illicit financial flows) and their Interpretive Notes

FCA – Financial Conduct Authority

FSMA – Financial Services and Markets Act 2000

GPG45 – Good practice guide 45 (for verifying identity)

HMRC – His Majesty's Revenue and Customs

HRTCs – High Risk Third Countries

IDV – Identity verification

JMLSG – Joint Money Laundering Steering Group

ML – Money Laundering

MLRs – The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (S.I. 2017/692)

NCA – National Crime Agency

NRA – National Risk Assessment of Money Laundering and Terrorist Financing

OPBAS – Office for Professional Body Anti-Money Laundering Supervision

PBS – Professional Body Supervisor

PCA – Pooled Client Account

PEP – Politically Exposed Person

PF – Proliferation Financing (of Weapons of Mass Destruction)

Regulated Activity -

Regulated Firm – used in this document to refer to any entity carrying out activities regulated under the MLRs. This can include individuals, such as barristers. Under the MLRs, it is often the 'relevant person' who is subject to the provisions, rather than the firm itself.

ROE: Register of Overseas Entities

SDD – Simplified Due Diligence

Supervisors – bodies responsible for supervising firms who are subject to the MLRs, including the Gambling Commission, HMRC, the FCA and the Professional Body Supervisors

TCSP – Trust and Company Service Provider

TF – Terrorism Financing

TRS – Trust Registration Service

HM Treasury contacts

This document can be downloaded from www.gov.uk

If you require this information in an alternative format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 5000

Email: public.enquiries@hmtreasury.gov.uk