HM Treasury

The draft Money Laundering and Terrorist Financing (Amendment and Miscellaneous Provision) Regulations 2025

Policy note

September 2025

HM Treasury

The draft Money Laundering and Terrorist Financing (Amendment and Miscellaneous Provision) Regulations 2025

Policy note

September 2025

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

Any enquiries regarding this publication should be sent to us at public.enquiries@hmtreasury.gov.uk

ISBN: 978-1-917638-53-1

PU: 3553

Contents

Chapter 1
Introduction and context

Background

1.1 Following a public consultation on 'Improving the Effectiveness of the Money Laundering Regulations'[1], the government is bringing forward targeted amendments to close regulatory loopholes, address proportionality concerns, and account for evolving risks in relation to money laundering and terrorist financing. The consultation highlighted specific weaknesses in the UK's regime, including issues with pooled client accounts, trust registration, cryptoasset business regulation, and the practicalities of customer due diligence.

1.2 This Statutory Instrument is one part of the government's response[2] to those concerns, aiming to deliver a more risk-based, proportionate regime that is robust against financial crime whilst remaining workable for industry. The government has also committed to improve sectoral guidance on AML/CTF compliance on a range of issues, and to publish separate guidance on the use of digital identity verification for AML/CTF purposes.

Purpose of this note

1.3 This policy note accompanies the draft Money Laundering and Terrorist Financing (Amendment and Miscellaneous Provision) Regulations 2025 ("the SI"), which is published alongside this note for technical consultation. The SI comprises amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) and related legislation.

1.4 HM Treasury invites feedback from regulated firms, supervisors, other government departments and interested stakeholders on the practical operability, clarity, and effectiveness of the draft provisions. This is a draft SI and should not be treated as final. It is being published for technical checks, such as any significant errors or oversights in the legal drafting that would mean that the provisions in this SI would not achieve the desired outcomes explained in this note, or that could lead to other significant unintended consequences. The drafting approach,

---

1 https://assets.publishing.service.gov.uk/media/65e9e1813649a2001aed6492/HM_Treasury_Consultation_on_Improving_the_Effectiveness_of_the_Money_Laundering_Regulations.pdf

2 https://assets.publishing.service.gov.uk/media/6878c1b42bad77c3dae4dd25/MLRs_Consultation_Response.pdf

and other technical aspects of the proposal, may therefore change before the final instrument is laid before Parliament.

Next Steps

1.5 This technical consultation is open for four weeks, closing on 30 September 2025. HM Treasury welcomes comments on the technical effectiveness and practical implementation of the SI, including any unintended consequences or areas of ambiguity. Subject to feedback and Parliamentary scheduling, the final instrument is expected to be laid in early 2026 and will come into force 21 days after being made, with specific provisions for cryptoasset businesses aligned to the commencement of the FSMA cryptoasset perimeter.

1.6 Responses should be sent to: Anti-MoneyLaunderingBranch@hmtreasury.gov.uk

Chapter 2

Summary of measures and policy intent

2.1 Below is a summary of the principal measures in the SI, each accompanied by its policy intent. Unless otherwise specified, references to regulations are references to regulations in the SI. The measures are grouped in this note according to the chapter of the consultation response in which they were set out.

Making customer due diligence more proportionate and effective

Customer Due Diligence (CDD) triggers for letting agents and art market participants (Regulations 13(f) and (h)(i))

Policy intent: Ensure CDD triggers are clear and consistent across all sectors.

- The SI aligns transaction-based CDD requirements for letting agents and art market participants with those for high value dealers.

Onboarding of customers in bank insolvency scenarios (Regulations 15, 16 and 17)

Policy intent: Facilitate continued access to banking services for customers following a bank or building society insolvency event, while maintaining AML safeguards.

- New provisions allow credit institutions, in specific circumstances following a bank insolvency, to verify the identity of customers from insolvent banks *after* account opening, providing ID verification is completed as soon as practicable.
- Use of this exception is subject to safeguards including that onboarding firms must notify the FCA so that it can supervise accordingly; the exception cannot be used for customers who would be subject to enhanced due diligence measures (i.e. who present a high risk of money laundering or terrorist financing); and use of the exception for personal customers is only permitted where the bank insolvency has led to a delay to ID verification timescales.

Enhanced Due Diligence

Policy Intent: Ensure enhanced due diligence measures are targeted, evidence-based, and proportionate, so that firms can focus their efforts

on the transactions and jurisdictions that present the greatest risk. This should improve the effectiveness of the UK's anti-money laundering regime, reduce unnecessary burdens on business, and ensure that resources are used where they have the greatest impact.

High-Risk Third Countries (Regulations 18(b) and 22)

- The SI updates when EDD is required in relation to a person or transaction linked to a specific country. Firms are currently required to apply EDD to transactions or customers involving "high-risk third countries", which is in turn defined as any country on the FATF's 'increased monitoring' *and* 'call for action' lists. The SI narrows this to focus specifically on "FATF call for action countries". i.e. only countries on the 'call for action' list. This ensures firms can direct their resources to jurisdictions which present the greatest risk to the UK.

Complex and large transactions (Regulations 10,11 and 18(a))

- The MLRs currently require firms to apply EDD to all "complex or unusually large" transactions. However, this wording leads to confusion and, in some sectors, an overly cautious approach.
- The SI clarifies that enhanced due diligence is required only for transactions that are "unusually complex or unusually large" relative to what is typical for the sector or the nature of the transaction. This change does not introduce a new obligation but rather refines the existing requirement to ensure that firms can focus their compliance efforts on transactions that present genuinely higher risks, rather than expending resources on routine transactions that do not warrant additional scrutiny.

Pooled Client Accounts (PCAs) (Regulations 14 and 20)

Policy intent: Increase the supply and accessibility of PCAs for businesses with a legitimate need, while maintaining robust risk-based controls.

- The SI decouples PCAs from the simplified due diligence (SDD) framework, removing the requirement for banks to treat PCAs as "low risk" or only offer them to AML/CTF-regulated customers.
- A new provision requires all financial and credit institutions to take reasonable measures to understand the purpose of the PCA, gather sufficient information about the customer's business, and assess the risk associated with the account. Banks must obtain further information and consider imposing additional controls on the PCA where appropriate to manage risk.
- Holders of PCAs must, on request, provide the bank with information about the identity of persons whose funds are held in the account (i.e. the underlying customers). This is intended to ensure transparency and facilitate effective oversight, without requiring banks to conduct CDD on all underlying customers.

Strengthening system coordination

Information sharing (Regulations 27, 28(b), 29 and 30)

Policy intent: Strengthen cooperation and information sharing between AML/CTF supervisors and other public bodies.

- The SI includes Companies House within the scope of the duty to cooperate obligations among AML supervisors, recognising Companies House's enhanced role as a gatekeeper for corporate transparency and as an integral part of the UK's AML supervisory framework.
- The SI adds the Financial Regulators Complaints Commissioner to the list of relevant authorities eligible for information sharing under the regulations, facilitating more effective cooperation and oversight in the AML framework.
- The SI makes two minor changes to MLRs Regulations 52A and 52B, which cover the disclosure by the FCA of confidential information relating to MLRs supervision. This expands the scope of confidential information which the FCA is empowered to share in the course of delivering its functions under the MLRs to include information about MLRs supervision of cryptoasset firms. The SI also amends the defence to the offence of breaching confidentiality obligations to align further with the defence for breaching the confidentiality restriction at s.348 of the Financial Services and Markets Act (FSMA).

Providing clarity on scope and registration issues

Currency thresholds and definitions (Regulations 4(b) and (c), 7, 8, 9(b), 13(a) to (e), (g), (h)(ii) and (j), 21, 32 and 33)

Policy intent: Simplify compliance by reducing conversion complexity and reflect UK market practice post-EU exit.

- The SI converts all monetary thresholds for customer due diligence, reporting, and transaction triggers from euros to sterling (e.g. €10,000 becomes £10,000), with some thresholds adjusted to ensure the UK continues to meet international standards set by the Financial Action Task Force.
- It also updates the general interpretation regulation in the MLRs to reflect these changes.

Regulation of sale of off-the-shelf companies by Trust and Company Service Providers (TCSPs) (Regulation 6)

Policy intent: Close a gap in the MLRs by ensuring that CDD is carried out across the full range of TCSP services.

- The SI brings the activity of selling "off-the-shelf firms" within the scope of regulated activities for TCSPs, meaning that TCSPs

selling off-the-shelf firms must now comply with MLRs obligations, including customer due diligence and ongoing monitoring.

Registration and change in control for cryptoasset service providers (regulations 31, 37 and 38)

Policy intent: Amend the registration and change in control thresholds for cryptoasset firms to align with thresholds in the Financial Services and Markets Act (FSMA), delivering consistency across the cryptoasset sector and ensuring owners of cryptoasset firms involving complex ownership structures are not missed from fit and proper checks.

- The SI amends the scope of fit and proper tests for cryptoasset businesses registered under the MLRs for the purposes of registration (Regulation 54(1A) of the MLRs) and change in control (Regulation 60(B) and Schedule 6B of the MLRs).
- Regulation 31 applies to registration and amends the fit and proper test to require the FCA to assess whether the applicant's controller (within the meaning of section 422 of FSMA) is a fit and proper person. This will replace the requirement for the FCA to assess the applicant's beneficial owner.

2.2 Regulation 31 will commence when the forthcoming FSMA cryptoasset authorisation regime comes into force[3]. The FCA would however continue to apply the fit and proper test to a beneficial owner where the cryptoasset business is registered under the MLRs before the new regime and the FCA is considering cancelling the registration under regulation 60 of the MLRs (regulation 38).

2.3 Firms authorised under FSMA will no longer need to register under the MLRs to avoid dual registration and reduce burden on firms. Registration under the MLRs for cryptoasset businesses will only apply to those who are not authorised under FSMA (those that meet the definition of a cryptoasset business under the MLRS but not under FSMA).

2.4 Regulation 37 applies to change in control, and substitutes a new Schedule 6B into the MLRs. For cryptoasset businesses registered with the FCA under the MLRs *before* FSMA comes into force, the SI will extend the category of persons required to give notice to the FCA for change of control. Beneficial owners will continue to be required to give notice, in addition to those who hold 10% or more of the shares or of the voting power, or can exercise significant influence over the management of the cryptoasset business.

For cryptoasset businesses registered with the FCA under the MLRs *after* the FSMA cryptoasset authorisation regime comes into force, the category of persons required to give notice to the FCA for change of

[3] See: https://www.gov.uk/government/publications/regulatory-regime-for-cryptoassets-regulated-activities-draft-si-and-policy-note

control will align with the FSMA controller definition to ensure alignment between the two regimes

Reforming registration requirements for the Trust Registration Service

Trust Registration Service (Regulations 23, 24, 25, 26 and 35)

Policy intent: Improve the effectiveness of the Trust Registration Service by closing loopholes that could be leveraged to obscure asset ownership, improving transparency of beneficial ownership of trusts with significant UK connections and refining registration requirements for other types of trust.

- The SI expands the categories of trusts required to register on the Trust Registration Service, bringing additional types of trusts within scope while introducing new exclusions for trusts that are low-value, low risk, inappropriate, or trusts related to estates administration.
- The SI extends both the requirement to provide beneficial ownership information and for this information to be accessible for these newly in-scope trusts: increasing the transparency of trusts that own or control UK assets.
- The SI removes the previous provision under which liability to Stamp Duty Reserve Tax (SDRT) automatically triggered a trust's registration requirement; as a result, trusts will no longer need to register solely on the basis of SDRT liability.

Proposed further MLRs revisions

Policy intent: Make additional minor and technical changes to the MLRs in order to ensure consistency, clarity and a risk-based approach.

- The SI clarifies and updates the exemptions for overseas sovereign wealth funds, specifying that funds operated by central banks or other public bodies are exempt from certain AML requirements, in line with international practice and risk assessments. **(Regulations 2 and 9a)**
- The SI explicitly excludes reinsurance contracts from the definition of "insurance undertaking" for AML purposes, ensuring that reinsurance activities are not subject to requirements intended for direct insurance providers. **(Regulation 5)**
- The SI inserts a new regulation 34A into the MLRs to require cryptoasset exchange providers and custodian wallet providers to apply enhanced due diligence in correspondent relationships. Correspondent relationships with shell banks are prohibited. This aligns UK requirements for cryptoasset businesses with FATF recommendations. **(Regulation 19)**

- The SI updates the list of recognised professional bodies to reflect recent organisational changes, ensuring that supervisory responsibilities and regulatory oversight remain current and accurate. **(Regulation 34)**
- The SI amends MLRs Regulation 23 so that FCA-supervised money service businesses or trust and company service providers which have provided the FCA with information under that regulation are required to report to the FCA any inaccuracies in that information. This aligns with equivalent provisions in the draft Financial Services and Markets Act 2000 (Regulated Activities and Miscellaneous Provisions) (Cryptoassets) Order 2025, and ensures that the FCA is kept up to date with relevant developments that may affect a firm's risk profile or compliance status. **(Regulation 12)**

Chapter 3

Processing of Personal Data

Data subjects

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

The personal data we collect

3.2 The personal data will be collected directly from data subjects through voluntary email submissions in response to this consultation and are likely to include respondents' names, email addresses, employers, job titles, telephone numbers, and opinions.

3.3 Respondents might include other types of personal data in their response to this consultation where they feel that it is relevant to their response.

How we will use the personal data

3.4 This personal data will be processed for the purpose of obtaining opinions about government policies, proposals, or an issue of public interest to inform the further development or implementation of the consultation subject.

3.5 Contact details you provide during this consultation will, in some circumstances, be used to contact you to discuss your response further.

3.6 Processing of this personal data is necessary to help us understand who has responded to this consultation and their opinion on the amendments to the MLRs instituted through the SI.

3.7 Consultation responses will be used to consider any appropriate amendments to the draft legislation.

Lawful basis for processing the personal data

3.8 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 continued development of the SI.

Who will have access to the personal data

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

3.10 There is no intention to share personal data collected during this consultation with any other data controllers.

3.11 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

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

Your data protection rights

3.13 You have the following rights in relation to this activity:

- 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.
- request that we restrict the processing of your personal data in certain circumstances.
- 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)

3.14 You can exercise your information rights - including requesting a copy of personal data that HM Treasury holds about you - by contacting DSAR@HMTreasury.gov.uk. You will not be charged to exercise your information rights.

3.15 You can help us to process your request more effectively by explaining what information you think HM Treasury holds about you.

3.16 We will usually need to verify your identity before we can provide you with personal data, as such, you can assist us in actioning your request quickly by providing:

- proof of identification (such as a copy of a passport or picture driving license) and
- proof of address (such as copy of a bank statement or utility bill).
- Please do not send original documents to us, copies or digital versions are sufficient.

Complaints

3.17 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

3.18 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 the ICO website.

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