Baker McKenzie.

Client alert

Alert | June 2019

New EU Rules on AML group-wide policies effective from 3 September 2019

What are the new requirements and when do they apply?

The European Commission has published new regulatory technical standards that apply specifically to credit and financial institutions, including e-money institutions, payment institutions, investment firms, AIFMs and UCITs Mancos. The new standards specify "additional measures" in respect of relevant institutions' branches and majority-owned subsidiaries ("Local Entities") operating outside the EEA. Where local law does not allow implementation of group-wide policies and procedures to effectively handle the risk of money laundering and terrorist financing, they will need to take "additional measures" proportionate to the level of risk and in the worst case stop carrying on business. The Commission is looking to achieve a more consistent EU approach with this initiative.

The new rules take effect on **3 September 2019** leaving firms with little time to prepare. As a minimum senior management and compliance now need to:

1. review AML/CTF risk in all non-EEA countries in which they have Local Entities, in order to identify those jurisdictions which have requirements that are less stringent than their home member EEA state or have restrictions that impact on AML/CTF controls;
2. take mitigating actions to reflect the restrictions or different standards applicable in those non-EEA countries; and
3. notify their home state regulator (for UK financial services firms, likely to be the FCA) of the relevant restrictions / standards.

The Commission's new rules come at a time when there is increasing focus on the importance of group-wide policies and procedures especially in the context of overseas operations of EEA businesses. Lax controls are seen as a potential "back door" to money laundering and terrorist financing. In this regard, earlier this year the Financial Conduct Authority brought a civil action under the 2017 Money Laundering Regulations against a financial institution that had failed to require its non-EEA branches and subsidiaries to apply UK-equivalent AML standards to customer due diligence and ongoing monitoring.

What are the current requirements for group-wide policies?

The Fourth Money Laundering Directive requires all regulated firms, including traditional banks and investment firms, FinTechs and other financial services businesses to put in place group-wide policies and procedures to address the risk of money laundering and terrorist financing. These should include data protection policies and procedures for sharing information within a group for these purposes. For Local Entities outside the EEA, where local AML/CFT requirements are less strict, to the extent that local law allows, the group should apply the standards of its home member state. For Local Entities within the EEA, there is an obligation under the Fourth Money Laundering Directive on firms to ensure that their Local Entities follow the law of that EEA state as it implements the Directive, but firms will also need to comply with their UK obligations.

The 2017 Money Laundering Regulations that transposed the Directive into UK law specify that groups should regularly review and update their policies, controls and procedures. Written records should be kept showing how they are communicated to staff in subsidiary undertakings and branches and any changes made to these policies, etc.

Where the local law of a non-EEA country does not allow the application of UK requirements, the group must inform its AML supervisor and take additional, but unspecified measures to combat AML/CTF risk. Ultimately, member state AML supervisors can require groups to terminate business relationships or even request that entire operations be closed-down.

What are the new requirements for banks and other financial institutions?

The Commission's regulatory technical standards now specify a range of additional measures that credit and financial institutions must take if they judge necessary. However, for all non-EEA countries where they have Local Entities (that are branches or majority owned subsidiaries) they must as a minimum:

- assess the money laundering and terrorist financing risk to their group in that country, record that assessment in writing, keep it up to date and retain it, should (in the case of the UK) the FCA call to see it;
- ensure the risk assessment is reflected appropriately in their group-wide AML/CTF policies and procedures;
- obtain senior management approval at group-level for the risk assessment and resulting policies and procedures; and
- provide targeted training to staff members in the non-EEA country to enable them to identify risk indicators ensuring that the training is effective (e.g. by testing their understanding).

These general obligations may seem duplicative to steps already required to be taken at group level to assess and manage money laundering and terrorist financing risk, but they require firms to ensure that they have considered sufficiently the risk posed specifically by the non-EEA country and the impact on the group as a whole.

Where banks and financial institutions identify that local law requirements impede policies and procedures necessary to identify and assess AML/CFT risk because they restrict or limit:

- the use of customer and beneficial ownership information for customer due diligence (CDD);
- the sharing or processing of customer data for AML/CTF purposes;
- the sharing of information on suspicious transaction reports with other entities in the group;
- the transfer of customers' data to the EEA for the purpose of AML/CTF supervision; or
- the putting in place of record-keeping measures equivalent to the Money Laundering Regulations;

the relevant UK firm must inform its AML supervisor (in the UK, the FCA) "without undue delay" but in any event within 28 calendar days of the identity of the country concerned and the nature of the issue. If relevant, they must investigate if consent can be obtained from beneficial owners and customers to overcome any restrictions on the use of their information and, in the case of suspicious transaction reports (STRs), provide senior management with sufficient statistical information regarding STRs made locally to have an overview of the position.

What are the specified "additional measures"?

Where any restrictions cannot be overcome banks and financial institutions must take additional measures to manage the AML/CTF risk. These depend on the nature of the restriction and risk but cover:

- only offering low risk financial products and services;
- ensuring that other entities in the group do not rely on CDD carried out on a customer by a local entity in that country;
- carrying out enhanced reviews such as onsite checks or independent audits to satisfy themselves that the local entity effectively identifies, assesses and manages the risk;
- ensuring the Local Entity seeks senior management approval at group level to establish and maintain higher-risk business relationships or carry out similar occasional transactions;
- determining the source and destination of funds to be used;
- ensuring the Local Entity carries out enhanced ongoing monitoring of the business relationship until they are reasonably satisfied they understand the risk associated with the business relationship;
- ensuring the Local Entity shares with the group information underlying suspicious transaction reports, including personal information to the extent possible under the country's law;
- carrying out enhanced ongoing monitoring on any customer and, where applicable, the beneficial owner of a customer who has been the subject of suspicious transaction reports by other entities in the same group;
- ensuring that the Local Entity has effective systems and controls to identify and report suspicious transactions; and
- ensuring the Local Entity keeps the risk profile and due diligence information on their customers up to date and secure as long as legally possible, and in any case at least during the business relationship.

What happens if "additional measures" are insufficient?

A group must take these additional measures on a risk-sensitive basis and be able to show their supervisor that they are effective. If it is still not possible to manage properly the AML/CTF risk, senior management must consider a range of options by the local entity from terminating the relationship, abstaining from occasional transactions or closing down part or all of that entity's operations. Quite what action to take depends on the risk posed.

Which non-EEA countries restrict or limit CDD?

The European Supervisory Authorities (ESAs) drafted these requirements and consulted on them in 2017. They wanted to achieve a consistent approach to identifying and managing third country risks by the EEA's financial sector. The delay in finalising and adopting them is explained in part by other financial crime priorities before the Commission and, as was evident during the consultation process, that very few third countries had been identified as impeding group-wide AML/CFT policies and procedures. To date, the Commission has still not provided a list of such countries; rather the burden rests on regulated firms to assess non-EEA countries and the AML/CTF environment in which their Local Entities operate. On the other hand, in response to the consultation, it was said that member state supervisors or the ESAs would consider whether certain information might be published (i.e. the countries where other firms have reported obstacles). In the meantime, a starting point for firms will be the Commission's list of high-risk third countries and the Financial Action Task Force's jurisdictions with strategic deficiencies.

Firms should, as a matter of urgency, be analysing the laws of the jurisdictions in which they have Local Entities to determine whether the obligations will be triggered under the technical standards to make regulatory notifications and take mitigating actions.

What's on the horizon?

Under the Fifth Money Laundering Directive that takes effect in January 2020, member states and ESAs, when assessing if non-EEA countries hinder proper implementation of group-wide policies, must expressly take account of any legal constraints, including: (1) secrecy (2) data protection and (3) other constraints limiting the exchange of information. This suggests that in future supervisors may regard a higher number of countries to be in this category by encompassing, for example, those jurisdictions that are non-cooperative in respect of tax and beneficial ownership. If Brexit occurs on 31 October 2019, these provisions will not automatically apply in the UK.

Should a hard Brexit take place on 31 October 2019 or on a later date, the UK will become a non-EEA country and from the point of view of the UK, EEA countries will similarly be third countries. The Money Laundering EU Exit Regulations (UK Exit Regulations) with respect to group-wide AML policies provide that UK parent companies will no longer need to ensure that Local Entities in an EEA state follow the law of that state (i.e. as it has transposed EU Money Laundering Directives). If an EEA state were judged not to impose requirements as strict as the UK, to the extent allowed by local law, a group would have to ensure their Local Entity applied measures equivalent to those under the UK Money Laundering Regulations. Again, this will require businesses to carry out a gap assessment and a study of what local law allows. Different conclusions may be reached depending on the EEA state - for example, if some EEA states are restrictive on data sharing. The UK Exit Regulations give the FCA power to make requirements specifying what additional measures and minimum action should be taken by banks and financial institutions when the law of a third country does not allow a Local Entity to apply UK equivalent measures. In practice, these would likely amend the EU's technical standards and might conceivably provide some relief for parent companies with Local Entities in EEA states. In the end, much may depend on the approach of supervisors.

Key action points for firms

The implementation deadline of 3 September 2019 is now less than three months away. Firms should if they have not already:

- carry out the minimum steps in non-EEA countries where there are Local Entities (i.e. a local written risk assessment that is reflected in group-wide policies approved by senior management, with staff receiving training);
- review non-EEA countries where there are Local Entities to assess whether local AML/CFT requirements are less strict and identify if there are any restrictions in applying UK requirements. This will necessarily include some legal review of the frameworks in those jurisdictions;
- where there are restrictions in applying UK requirements inform the FCA "without undue delay", but in any event within 28 calendar days of the country concerned and the nature of the issue;

- if the restriction cannot be resolved (e.g. obtaining consent from customers where applicable), consider applying specified "additional measures" on a risk-sensitive basis;
- consider options ranging from terminating business relationships to ceasing the whole or part of operations in the country if the application of additional measures is insufficient to manage the risk; and
- be ready to demonstrate to AML supervisors that their assessments and steps taken are appropriate and have been fully documented.

Contact us

Mark Simpson
Partner
mark.simpson
@bakermckenzie.com

Caitlin McErlane
Partner
caitlin.mcerlane
@bakermckenzie.com

Philip Annett
Partner
philip.annett
@bakermckenzie.com

Richard Powell
Knowledge Lawyer
richard.powell
@bakermckenzie.com