Fraud and working with your MLRO

Money laundering risk remains a priority for the government and regulators because of the sheer scale of the problem. The clandestine nature of illicit transactions makes it difficult to put an accurate number on the value of money laundered globally, however, the United Nations Office on Drugs and Crime estimates the figure to be between $800bn and $2trn every year, or 2–5% of global gross domestic product.

Responding to an alleged scheme originating in Russia that involved the 'cleaning' of some £65bn in assets, £600m of which is understood to have been routed through UK banks, the Economic Secretary to the Treasury, Simon Kirby, told parliament in 2017 that the "government will do what it takes" to crack down on such activity. "We need to ensure that sophisticated criminal networks cannot exploit our financial services industry," he added.

As recognised in the second National Risk Assessment report, the UK's financial services sector is a major global hub that attracts investment from across the world. Its size and openness also make it attractive to criminals seeking to hide the proceeds of crime among the huge volumes of legitimate businesses.

This vulnerability to such abuses has prompted a heightened regulatory response, the Financial Conduct Authority (FCA) is stepping up its efforts to reduce poor money laundering practices by issuing heavy penalties. In January 2017 the regulator fined Deutsche Bank £163m for not maintaining an adequate anti-money laundering (AML) framework between 2012 and 2015, the largest fine ever issued in the UK for such a failure.

Legislative oversight has also increased, and this applies to various sectors, not just financial services. On June 26 2017 the UK implemented the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (MLR 2017), replacing and increasing the scope of the pre-existing Money Laundering Regulations 2007 (MLR 2007).

The new law applies to all sectors previously covered by MLR 2007, therefore the following types of organisations, and their internal audit functions, should already be familiar with their pre-existing AML responsibilities:

- Credit institutions
- Financial institutions
- Auditors, insolvency practitioners, external accountants and tax advisers
- Independent legal professionals
- Trust or company service providers
- Estate agents
- High value dealers
- Casinos

It is important to note that if you are the chief audit executive (CAE) for an online gambling provider, your company will be covered by MLR 2017, whereas MLR 2007 only applied to holders of casino licences.

Every business covered by the regulations must be monitored by a supervisory authority.

All banks and other regulated financial institutions are under the FCA's supervision, while gambling operators are supervised by the Gambling Commission. If your organisation is a member of a professional body, such as the Law Society or ICAEW, that body will act as your organisation's supervisor (a full list of professional bodies with supervisory powers are listed here). Any other organisations regulated by MLR 2017 fall under the watch of HMRC.

Every organisation, including their CAEs, should keep abreast of guidance developments issued by their respective supervisors, which are required by law to conduct sector-specific money laundering risk assessments.

There are many similarities between MLR 2017 and its predecessor, MLR 2007, and the intention was not to tear up the rulebook and start from scratch but make the law more comprehensive. There are, however, notable changes.

It is essential, therefore, that financial institutions and other regulated organisations comply with MLR 2017 to avoid significant fines and even prosecution; under the new law, anyone who makes a false or misleading statement in the context of money laundering can be imprisoned for up to two years.

MLRO and compliance

The money laundering reporting officer (MLRO), a role introduced under previous legislation, is responsible for supervising the organisation's AML compliance, staff training, disclosing Suspicious Activity Reports (SARs) to the National Crime Agency (NCA), and advising on how to proceed with activities following a SAR in order not to prejudice an investigation or tip off a potential offender.

Since MLROs have ultimate responsibility for supervising the organisation's AML compliance, they will have to consider the changes brought into effect by MLR 2017.

Let's consider some of those changes:

Compulsory risk assessments

One of the defining characteristics of the law is its emphasis on risk-based approaches and the first step will be to conduct a comprehensive risk assessment. This is a compulsory measure and entails producing a written AML risk report that takes into consideration customers, countries of operation, products and services, transactions, delivery channels and the size and nature of the business. The organisation must then translate the findings of this process into written risk-based policies and controls.

This requirement also applies to the government, which has already completed its National Risk Assessment (link above) to identify and mitigate the risks of money laundering and terrorist financing in the UK, and the supervisory authorities according to their supervised sectors (see above).

What policies?

These policies must be codified, commensurate with the risks identified in the risk assessment and signed off by senior management. In essence, policies should be designed to identify and bring under closer scrutiny any complex or unusually large transactions or series of transactions, or otherwise draw attention to activity that may reasonably indicate money laundering or terrorist financing.

There are reporting, record keeping and monitoring requirements for compliance efforts and the law also

calls for an appointed money laundering compliance principal (MLCP) who is also a member of the board or senior management, although this can be the same person as the already designated MLRO if they are sufficiently senior. Any staff whose work is relevant to AML compliance must also be appropriately screened and trained.

Crucially, MLR 2017 states than an “independent audit function” should be established to assess the adequacy and effectiveness of the firm’s AML policies, controls and procedures. This should already be the case for any CAE reading this briefing, but the stipulation drives home the expectation that audits are performed to ensure the organisation is compliant and to offer a second, independent opinion on the efficacy of AML risk mitigation measures.

Heightened due diligence

Due diligence has become more onerous under MLR 2017. Where previously banks and other organisations could automatically apply 'simplified due diligence' providing a business relationship or transaction met specified criteria, this can now only be applied once a number of risk factors have been considered and it has been determined that there is a low risk of money laundering and terrorist financing.

These factors include whether the customer is a credit institution or financial institution which is subject to the EU's Fourth Money Laundering Directive (the directive that sets the framework for MLR 2017) and is located in a high-risk geography blacklisted by the European Commission. Controversially, in February 2018 the European Parliament closely voted that Tunisia, as well as Sri Lanka and Trinidad and Tobago, should be added to the blacklist. (At the time of writing this blacklist had not been updated. The previous version is available here. If a relationship or transaction presents a high degree of risk, enhanced due diligence and risk assessment are compulsory.

Politically exposed persons

A PEP is someone entrusted with a prominent public function and who, therefore, presents a higher bribery and corruption risk due to their power and influence. PEPs may be able to misappropriate public funds and launder kickbacks. MLR 2017 expands the scope to include UK as well as foreign PEPs. This will mean extending enhanced due diligence to a longer list of higher-risk individuals such as heads of state, ministers, members of parliament, supreme court judges, the board members of international organisations and their immediate family members or known associates.

Third party requirements

Organisations are still permitted to rely on the customer due diligence carried out by third parties, as long as those third parties are subject to the MLR 2017 or an equivalent regime. However, MLR 2017 is stricter in that it requires third parties to enter into written agreements under which they are obliged to provide all customer due diligence materials that relate to the customer and any related beneficial owners.

A beneficial owner is anyone who has a direct or indirect shareholding of 25% or more of a company, or otherwise has significant control over the company without being its legal owner.

A risk-based approach

Given the extent to which financial services are globalised and highly regulated, UK banks and other regulated organisations will not just have to consider MLR 2017 but a raft of requirements in various

jurisdictions. At the heart of all AML laws and regulations, however, is the common-sense principle of knowing your customers. This applies to all sectors with significant exposure to money laundering and requires a risk-based approach, such that transactions and customers that pose the highest risk of money laundering and terrorist financing are given the most attention.

Red flags include customers and transactions originating from high-risk countries, PEPs, sanctioned organisations, complex and unusually large transactions, or ones without any apparent legal or economic purpose. If it looks suspicious then there's a good chance that it is.

Ten key questions

For CAEs seeking to assess the organisation's compliance with MLR 2017 and, at a more fundamental level, the effectiveness of money laundering risk management by the second line of defence, we suggest that audits seek to answer the following:

1. Is there a MLRO and are they of a sufficiently senior standing (i.e. a member of 'senior management') to adopt the MLCP role?
2. Is the MLRO confident that the organisation is compliant with MLR 2017 and can they provide evidence to back this up? Does record-keeping show that compliance is being effectively monitored by the MLRO?
3. Is the MLRO up to date with guidance issued by the organisation's supervisory authority (e.g. the FCA)?
4. Has a compulsory risk assessment been conducted? Is there evidence to support the robustness of the methodology of the assessment? Is internal audit confident that the assessment is accurate?
5. Are updates to controls and processes commensurate with the risk assessment, i.e. do controls mitigate the risks identified in the assessment?
6. Has customer due diligence been updated so that processes are only simplified once it is determined customers are not high risk, in keeping with MLR 2017's requirements?
7. Where the organisation relies on third parties for customer due diligence, are written agreements with those third parties in place?
8. Are all relevant staff aware of what suspicious transactions or customers look like, and are they familiar with local and foreign PEP lists, high-risk countries as well as sanctioned terrorist organisations?
9. Do relevant staff feel that they have been adequately trained and is that training appropriate to mitigate the money laundering risks unique to the organisation?
10. Has the reporting of any SARs to the NCA by the MLRO been conducted in a timely manner? Are there good reasons for why any suspicious activity reported to the MLRO by staff has not been submitted to the NCA? Are there any SARs backlogs and, if so, why?

Further reading

UK government's compulsory AML National Risk Assessment
FCA's overview of MLR 2017 including examples of risk-based approaches to AML