LexisNexis®

Practice Compliance anti-money laundering & counter-terrorist financing update: June 2017 implementation date

The Future of Law. Since 1818.

LexisNexis®

Practice Compliance anti-money laundering & counter-terrorist financing update: June 2017 implementation date

26 June 2017 is the deadline for law firms to have their new anti-money laundering systems in place. There is no current suggestion of a phased approach to implementation and the potential repercussions are onerous including hefty fines or prison sentences. Is your firm ready?

The proposed changes to the UK's overall anti-money laundering and counter-terrorist financing regime is the most significant change to our anti-money laundering and terrorist finance regime in over a decade, bringing additional administrative requirements with which law firms will need to ensure compliance.

The Government consultation on the draft Money Laundering Regulations 2017 (MLR 2017) closed on 12 April 2017. At the time of writing, there's no sign of the final regulations despite the fact that they're due to be implemented in less than a month.

It's highly unlikely, at this late stage, that MLR 2017 will be deferred notwithstanding the distraction of a snap general election, as the deadline for implementing the EU Fourth Money Laundering Directive expires on 26 June. With Parliament dissolved on 3 May, we may not see the final regulations until late June.

There's also radio silence from the Law Society on when we might expect a new or substantially AML amended practice note. The financial services sector is, however, leading the way—on 21 March 2017 the Joint Money Laundering Steering Group (made up of financial services trade associations) published for consultation its guidance which has been updated in line with the MLR 2017. The revised JMLSG guidance provides us with an indication of the direction the Law Society may well take with its own guidance.

In the meantime, we're in the process of growing and updating our AML content to reflect the new Regulations and subscribers are kept updated via Monthly Highlights and daily email alerts.

In this overview guide we set out Lexis®PSL Practice Compliance Practice Notes on the *Money Laundering Regulations 2017—what's changed for law firms?* and the *Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017—for law firms* based on the draft regulations.

Money Laundering Regulations 2017—what's changed (law firms)?

This Practice Note sets out new or amended provisions introduced by the Money Laundering Regulations 2017 (MLR 2017) as compared with the Money Laundering Regulations 2007 (the 2007 Regulations). References to Regulations are to the draft MLR 2017 except where indicated.

Headline changes for law firms to note include those in relation to:

- scope and application
- risk assessment
- client due diligence *(CDD), specifically:*
  - > reliance
  - > existing clients
  - > company formations
  - > simplified due diligence (SDD)
  - > equivalent jurisdictions
  - > politically exposed persons (PEPs)
  - > enhanced due diligence (EDD)
  - > persons acting on behalf of clients
- beneficial ownership
  - > definitions
  - > beneficial ownership information
- data protection
- systems and controls, eg:
  - > board level responsibility
  - > Nominated Officer
  - > employee screening
  - > internal audit function
  - > response systems
  - > group-level policies and procedures, and
- training

Scope and application

The scope and application of the MLR 2017 haven't changed significantly for law firms. They still apply where you are an independent legal professional, by way of business, participating (assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction) in financial or real estate transactions concerning:

- buying and selling of real property or business entities
- managing of client money, securities or other assets
- opening or management of bank, savings or securities accounts
- organisation of contributions necessary for the creation, operation or management of companies
- creation, operation or management of trusts, companies, foundations, or similar structures

The MLR 2017, however, increase the total annual turnover threshold below which the MLR 2017 do not apply from £64,000 to £100,000, subject to other factors (eg financial activity is only occasional, is not the main activity of the business, is very limited, etc). (MLR 2017 Reg 15)

They also bring high value dealers and the gambling industry into scope.

Risk assessment

The MLR 2017 are much stronger than their predecessor in terms of risk assessment in two senses:

- firm-wide risk assessment, and
- assessing individual client/matter risk

Firm-wide risk assessment

While the 2007 Regulations required you to take a risk-based, proportionate approach to your systems and controls, the MLR 2017 go further (Regulation 18). They contain a positive requirement for you to carry out a firm-wide assessment of the risk of money laundering and terrorist financing your business faces. They set out the sort of risk factors you must include.

You're going to have to make a written record of your risk assessment and make it available to the Law Society on request.

Matter risk assessment

Your CDD processes must reflect both your firm-wide risk assessment **and** your assessment of the level of risk arising in any particular case (ie the client/matter risk) (Regulation 28 (12)-(13).The MLR 2017 set out some factors you should be taking account of, ie:

- the purpose of the matter
- the size of the matter, and
- the regularity and duration of the business relationship

Client due diligence

There are quite a number of changes to CDD provisions, including in relation to:

- reliance
- existing clients
- company formations
- simplified due diligence (SDD)
- politically exposed persons (PEPs)

Reliance

There's a new time-frame in which you must provide documents to a third party relying on you if requested—at the latest, two working days (still subject to consultation) (Regulation 39(6).

There's been a significant expansion of the third parties which can be relied on, including all entities subject to the MLR 2017 (Regulation 38 (3)).

The MLR 2017 make it clear that you can use outsourcing providers to conduct CDD on your behalf, although of course you remain liable for any failure (Regulation 38(7)).

And, possibly most significant of all, where you rely on a third party you must now enter into written arrangements with that third party which enable you to obtain copies of any relevant documents and require the third party to retain those documents for the period specified in Regulation 39 (essentially 5 years—see Practice Note: Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017—for law firms). We'll be producing a Precedent in due course. (Regulation 38(2)(b)).

Existing clients

The MLR 2017, for the first time, set out general factors which would prompt the need for firms to re-apply CDD to existing clients (basically a summary of those contained in Annex I of 4MLD), (Regulation 27(7)) ie any:

- indication that the identity of the client (or its beneficial owner) has changed
- transactions which are not reasonably consistent with the firm's knowledge of the client
- change in the purpose and intended nature of your relationship with the client
- other matter which might affect your assessment of the money laundering or terrorist financing risk

The government says it expects sector-specific supervisors, in our case the Law Society, to set out more detailed guidance.

Company formations

The MLR 2017 contains the clarification that when a trust or company service provider is asked to form a company, this is to be treated as a business relationship (and is therefore caught by the MLR 2017) regardless of whether the formation is the only transaction being carried out for the client (Regulation 4(2)).

This is an area where the government continues to seek views. In its consultation the government asks under which circumstances it might be appropriate as part of the risk-based approach to apply SDD where the matter involves setting up a single corporate entity.

Simplified due diligence

The list of products and types of client that could be subject to SDD set out in the 2007 Regulations is not included in MLR 2017, so there's no automatic SDD anymore. Instead, the MLR 2017 include a non-exhaustive list of risk factors (following the non-exhaustive list set out in Annex II to 4MLD) which you should use to determine the risk posed by the client/matter and apply appropriate CDD from there. The government expects more detailed examples to be set out in sector-specific guidance. (Regulation 36(3)).

Pooled accounts have been a real bone of contention throughout the legislative process and it appears we are still no closer to reaching a consensus. So the position for now is that pooled accounts are not automatically subject to SDD, rather they are subject to the risk-based approach, and that is currently reflected in the MLR 2017. The government continues though to seek views on its approach to pooled accounts so watch this space. (Regulation 36(4)).

Equivalent jurisdictions

The concept of equivalence has bitten the dust. The EC will instead publish a list of high-risk third countries and you'll need to apply enhanced due diligence (EDD) in relation to any transaction or client established in one of those countries. Plus you won't be able to rely on a third party for CDD purposes who is established in them. (Regulations 33(3) and 38(4)). Here's the most up-to-date list.

Politically exposed persons

You also have to apply EDD to PEPs.

The MLR 2017 expand the PEP definition to those holding a politically exposed position in the UK. (Regulation 35)

The Financial Conduct Authority (FCA) is currently consulting on guidance (which it is required to provide under FSMA 2000, s 333U/Regulation 47, MLR 2017) on the treatment of PEPs, including in relation to lower-risk PEPs.

Subject to this guidance, senior management PEP approval is now required for any continuation of a PEP relationship as well as for setting those relationships up. You'll need to set out in your procedures the situations which will trigger the need for approval. (Regulation 35(5)).

Meanwhile a directive amending 4MLD (5MLD) is progressing through the European legislative process. 5MLD proposes a distinction between low-risk domestic PEPs and other PEPs so that firms could apply regular due diligence measures (as opposed to enhanced due diligence) to low-risk PEPs. The government says it will transpose this amendment if and when it makes it to publication in the Official Journal, so in the meantime you will need to conduct full-fat EDD to all domestic PEPs regardless of whether you consider them to be low or high risk.

Other enhanced due diligence requirements

As has always been the case, you must apply EDD measures where there is a higher risk of money laundering or terrorist financing.

But in addition to the usual suspects, the MLR 2017 also require you to apply EDD where:

- the client has provided false or stolen identification—query your ethical duties here, ie should you be acting at all, (Regulation 33(1)(e) and
- where the matter involves non-face-to-face business relationships unless certain safeguards are adopted, eg electronic signatures—this appears to be a relaxation of the 'physical presence' notion in the 2007 Regulations which may open the door to more modern ways of doing business like clients met via video call (Regulation 33(6)(b)(iii)

The MLR 2017 very helpfully set out factors you should consider to present a higher risk and which may therefore require EDD to be applied. (Regulation 33)

Persons acting on behalf of clients

There's a new requirement to verify that a person acting on behalf of a client (eg a signatory) is in fact authorised so to act, to identify them, and verify their identity. (Regulation 28(10)).

Beneficial ownership

Definition

The beneficial ownership definitions in the MLR 2017 are broadly the same as under the 2007 Regulations, except that they contain more detailed provisions in relation to trusts—specifically pulling the settlor and trustees into the definition of beneficial owner (Regulations 5-6).

Beneficial ownership information

4MLD requires member states to hold adequate and accurate information on beneficial ownership of corporate and other legal entities in a central register which would be available to specific authorities and those with a legitimate interest. This is a whole new part in the MLR 2017—Part 5.

The 'people with significant control' regime (PSC regime) was introduced for corporate entities through the Small Business, Enterprise and Employment Act 2015, but the government accepts it needs tweaking. It has consulted on what type of entity should be included in the PSC regime and how the register should be updated. It's still analysing responses.

We've been a little slower to legislate in terms of a beneficial ownership register for trusts, but the government is due to launch its register in summer 2017.

So this is one to watch. The MLR 2017 is clear though that you will **not** satisfy CDD requirements in relation to beneficial ownership simply by relying only on the information contained in these central registers. (Regulation 28(9)).

Data protection

The MLR 2017 introduce new requirements in relation to data protection (Regulation 40). These are:

- you can only process personal data obtained to comply with the MLR 2017 for the purposes of preventing money laundering and terrorist financing, ie you cannot obtain personal data for anti-money laundering (AML) purposes and then process it for something else, eg marketing
- you must provide new clients with the following information before establishing a business relationship or entering into an occasional transaction:
  - your registrable particulars under Data Protection Act 1998 (DPA 1998), ie:
    - > your name and address
    - > whether you have nominated a representative under DPA 1998
    - > a description of the personal data being or to be processed and the category or categories of data subject to which it relates
    - > a description of the purpose(s) for which it is being processed
    - > a description of any recipient(s) to whom you intend or may wish to disclose the data
    - > the name/a description of any countries outside the EEA to which the data may be transferred, and
  - a statement that any personal data received from the client will be processed only for the purposes of preventing money laundering and terrorist financing or as otherwise permitted

Systems and controls

Five headline changes in relation to general systems and controls:

- board level responsibility
- Nominated Officer
- employee screening
- independent audit function, and
- response systems

All are subject to proportionality, ie appropriate in relation to the size and nature of your business.

Board level responsibility

The MLR 2017 require you to appoint a member of the board (or equivalent) to be the officer responsible for your compliance with the MLR 2017 and inform the Law Society of the identity of that person and of any changes to the holder of the role. This appears to be in addition to the Nominated Officer appointment, although if your Nominated Officer is a board member, presumably you would tick both boxes. (Regulations 21(1)(a) and 21(4)).

Nominated Officer

Regulations 21(3) and 21(4) - Not only do you have to appoint a Nominated Officer (or MLRO) under the MLR 2017—familiar territory—but you also have to inform the Law Society of:

- their identity, and
- any changes to the holder of the role

Employee screening

Regulations 21(1)(b) - You must carry out screening (assessing the skills, knowledge, expertise, conduct and integrity) of employees or agents whose work is:

- relevant to your compliance with the MLR 2017, or
- otherwise capable of contributing to AML and counter-terrorist risk assessment or risk management, or the prevention or detection of money laundering or terrorist financing in relation to your business—the MLR 2017 do not contain any suggestions on who this might include

Independent audit function

The MLR 2017 require you to establish an independent audit function to:

- examine and evaluate the adequacy and effectiveness of your systems and controls
- make recommendations in relation to those systems, and
- monitor your compliance with those recommendations

There's no further explanation in the MLR 2017 (Regulation 21(1)(c)).

Response systems

The requirement in the 2007 Regulations for credit and financial institutions to have systems in place to enable full, rapid responses to investigators and other enforcement officers has been extended by MLR 2017 to include all businesses caught by the MLR 2017 (Regulation 21(8))

Group-level policies and procedures

The MLR 2017 introduce the concept of group policies. If you're a parent undertaking, you must ensure all your systems and controls apply to all your subsidiaries and branches (wherever located in the world) and that you have procedures for data protection and sharing information for the purposes of anti-money laundering and counter-terrorist financing. (Regulation 20)

Training

Regulation 24 - Your training must now:

- include agents as well as employees, and
- cover the law relating to data protection (presumably only insofar as it is relevant to AML)

The MLR 2017 also set out factors you must take account of in determining which training measures are appropriate for your business.

And, of course, you'll need to start thinking about how you'll train staff on the MLR 2017 and your shiny new (or at least significantly revised) policies and procedures.

What are we waiting for?

The MLR 2017 are still in draft format with a very short consultation period, which closed on 12 April 2017.

We're also waiting on the Law Society. We know it will need to make changes to its AML practice note and have the new version of its practice note approved by HM Treasury.

We're also waiting for guidelines from the FCA on how to treat PEPs and for European Supervisory Authorities (ESAs) to publish risk factor guidelines.

We're hoping not too much will change in terms of the MLR 2017 themselves. As to the ESAs and FCA guidance and Law Society practice note, things are far from certain. The Law Society has given no indication as to whether it will be an overhaul or a 'tweak where necessary' exercise.

In the meantime we'll be busy updating our AML and counter-terrorist financing content so we're ready when the UK government, ESAs, FCA and the Law Society are.

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017—for law firms

This Practice Note discusses the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (currently in draft) which will form part of the UK's overall anti-money laundering and counter-terrorist financing regime. The Regulations will come into force on 26 June 2017 and will give effect to the Fourth Money Laundering Directive. They set administrative requirements which run parallel to the criminal element of the AML and counter-terrorist financing regime contained in the Proceeds of Crime Act 2002 and the Terrorism Act 2000. There is some overlap. References below are to the draft Regulations unless otherwise indicated)

For more on POCA 2002 and the TA 2000, see Practice Notes: Proceeds of Crime Act 2002 and Counter-terrorist financing.

Application

The MLR 2017 apply to relevant persons acting in the course of business in the UK (***Regulation 8***). Relevant persons are:

- 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, and
- casinos

Subject to some exclusions, the following definitions, which may be relevant to law firms, apply (Regulations 11, 12):

Independent legal professionals	A firm or sole practitioner who by way of business provides legal or notarial services to other persons, when participating in (ie assisting in planning or execution of transactions or otherwise acts for or on behalf of a client) financial or real property transactions concerning: - buying and selling of real property or business entities - managing client money, securities or other assets (this is narrower than handling them) - opening or managing bank, savings or securities accounts (this is wider than simply opening a solicitor's client account) - organising contributions necessary for creating, operating or managing companies - creating, operating or managing trusts, companies, foundations or similar structures
Trust or company service provider	A firm or sole practitioner who by way of business provides any of the following services, when they provide such services: - forming companies or other legal persons - acting, or arranging for another person to act as director, secretary, partner, trustee, nominee shareholder or similar - providing a registered office, business address, correspondence or administrative address or other related services for a company etc
Tax adviser	A firm or sole practitioner who by way of business provides advice about the tax affairs of other persons, when providing such advice

Insolvency practitioner	Any person who acts as an insolvency practitioner within the meaning of section 388 of the Insolvency Act 1986

The MLR 2017 apply to lawyers when they are providing any of the above services. They **do not** apply where services other than those contained in the table above are being provided, eg:

- receiving payment of or on account of costs
- providing legal advice
- participating in litigation or any form of alternative dispute resolution
- will writing (but consider whether any tax advice is involved)
- publicly funded work

If you only provide services that do not fall within the scope of the MLR 2017, they do not apply to you. Note, however, that POCA 2002 and TA 2000 still apply—see Practice Notes: Proceeds of Crime Act 2002 and Counter-terrorist financing.

If you undertake activities which fall both within and outside the scope of the MLR 2017, they will only apply to the services you provide which fall within the scope of the MLR 2017. However, it is expected that most such firms will choose to apply MLR 2017 requirements across their entire business.

We'll be publishing a new Practice Note (MLR 2017—application) shortly.

Risk assessment

Despite many aspects of the substantive AML and CTF regime being 'risk-based', risk assessment did not feature prominently in the MLR 2007. The MLR 2017, however, contains an entire chapter dedicated to risk assessment and controls (Chapter 2) which begins with obligations on the government and supervisory authorities to conduct risk assessments. (Regulations 16-25)

The MLR 2017 then move on to relevant persons—that's you. (Regulation 18) You must take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which your business is subject, taking into account:

- information made available by supervisory authorities (the Law Society, in the case of solicitors)
- risk factors including those relating to:
  - your clients
  - the geographic areas in which you operate
  - your services
  - your transactions
  - your delivery channels
- the size and nature of your business

You must keep an up-to-date written record of all the steps you've taken and provide that record to the Law Society on request—see Precedents: Money laundering and terrorist financing—firm risk assessment—long form and short form.

Once you've identified the risks you face, you must establish and maintain systems and controls to mitigate and manage those risks—see: Policies and procedures below.

But your risk assessment obligations don't end there. Regulations 28(12)-(16) state the Client Due Diligence (CDD) measures you take must reflect:

- the firm-wide risk assessment you carry out, and
- your assessment of the level of risk arising in any particular case

In assessing the level of risk a client presents, you must take account of:

- the purpose of the business relationship
- the size of the transaction
- the regularity and duration of the business relationship

Note that you must be able to demonstrate to the Law Society that the extent of the measures you've taken is appropriate in view of the risks, including risks identified by you and the Law Society.

For more on risk assessment, see Subtopic: AML & counter-terrorist financing—Risk assessment, particularly Precedents: Client due diligence risk assessment form and Client due diligence risk tables.

Policies and procedures

Regulation 19 says that you must:

- establish and maintain policies and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing you identify in your firm-wide risk assessment which are:
  - > proportionate to the size and nature of your business, and
  - > approved by your senior management
- maintain a written record of the policies and procedures you establish

Your policies and procedures will include those in relation to:

- risk assessment
- internal controls including monitoring compliance with those controls
- CDD
- reporting suspicions
- record-keeping (including data protection)
- internal communication and training

Risk assessment

See above: Risk assessment.

Internal controls

Regulations 19-21 say that you must have policies and procedures which:

- provide for the identification and scrutiny of certain transactions/relationships
- specify additional measures to take in relation to transactions/relationships which might favour anonymity
- ensure appropriate measures are taken to assess and mitigate any risks caused by adopting new technology
- apply to all your subsidiaries and branches including those located outside the UK
- where appropriate, taking into account the size and nature of your business, provide for:
  - > the appointment of a senior individual to be responsible for compliance
  - > the screening of relevant employees and agents both before appointment and at regular intervals during the course of the appointment
  - > the establishment of an independent audit function
- enable you fully to respond to enquiries from law enforcement agencies

You must also appoint a nominated officer (unless you are a sole practitioner and do not employ any staff) who must receive suspicious activity reports from staff and determine whether they give rise to knowledge or suspicion of money laundering or terrorist financing—see Subtopic: Reporting suspicions.

We'll be publishing a new Practice Note (MLR 2017—systems and controls), which will set out more details, and further Precedents shortly.

Client due diligence

See below: Client due diligence.

Reporting suspicions

See subtopic: Reporting suspicions.

Record keeping

Record keeping requirements are not subject to the risk-based approach and therefore there is no room for subjective assessment of the extent to which you should comply (Regulation 39). You must keep the following records:

- a copy of CDD records
- sufficient supporting records (originals or copies) in respect of a matter to enable the transaction/matter to be reconstructed

You must retain them for five years:

What docs?	In what context?	Starting when?
Records, documents or information relating to an occasional transaction	Occasional transaction	Date you know or have reasonable grounds to suspect the transaction is complete
Records, documents or information relating to: - any transaction occurring as part of a business relationship, or - CDD measures taken in connection with that relationship	Business relationship	Date you know or have reasonable grounds to suspect the business relationship has come to an end
A copy of any documents and information obtained to satisfy CDD requirements	Where you are relied on by another relevant person	Date on which you are relied on

Once the five years are up, you must delete any personal data held, subject to some exceptions.

We'll be publishing a new Practice Note (MLR 2017—record keeping), which will set out more details, and further Precedents shortly.

Data protection

You can only use personal data obtained under the MLR 2017 for the purpose of preventing money laundering and terrorist financing, ie you cannot collect data for MLR 2017 purposes and then use it for something else. (Regulation 40). The only exceptions are where:

- use of the data is permitted under another piece of legislation, or
- you have obtained the express consent of the data subject

You must provide new clients with the following information before establishing a business relationship or entering into an occasional transaction:

- your registerable particulars under section 16(a) of the Data Protection Act 1998 (DPA 1998), ie your name and address, and
- a statement that any personal data received from the client will be processed only for the purposes of preventing money laundering and terrorist financing, or as permitted above (another piece of legislation or consent)

See further Practice Note: AML and data protection (law firms).

Internal communication and training

Where relevant, you must communicate your policies and procedures to branches and subsidiaries located outside the UK (Regulations 19(6) and 24).

You must take appropriate steps to ensure relevant employees and agents are:

- made aware of the law relating to money laundering and terrorist financing
- regularly given training on how to recognise and deal with matters which may involve money laundering or terrorist financing

We'll be publishing a new Practice Note (MLR 2017—systems and controls), which will set out more details, and further Precedents shortly.

Client due diligence

Regulations 4 and 27 say that you must apply CDD measures:

- where you establish a business relationship, ie:
  - > a commercial relationship which is connected to your business and which you expect at its inception to have an element of duration, or
  - > a relationship where you're asked to form a company for the client
- where you carry out an occasional transaction:
  - > that amounts to a transfer of funds exceeding €1000, or
  - > that amounts to €15000 or more in a single or multiple linked operations
- where you suspect money laundering or terrorist financing
- where you doubt the veracity or adequacy of documents or information you've previously obtained for CDD purposes
- at other appropriate times to existing clients on a risk-sensitive basis, taking into account:
  - > any indication that the identity of the client or its beneficial owner has changed
  - > any transactions which are not consistent with your knowledge of the client
  - > any change in the purpose or intended nature of your relationship with the client
  - > any other matter affecting your risk assessment of the client
- if you become aware that the circumstances of an existing client have changed and this is relevant to your risk assessment of that client

CDD is a vast and significant ingredient of the MLR 2017 and is covered in far greater detail in subtopic: Client due diligence, which contains guidance and a number of practical tools. The following is a summary of the headline elements of CDD.

Beneficial ownership

Beneficial ownership is complicated both in theory and in practice and was a significant bone of contention as 4MLD was thrashed out at EU level. There's a lot to say on it—it commands two introductory regulations in Part 1 of the MLR 2017 and its very own part; Part 5.

We'll be publishing a new Practice Note (MLR 2017—beneficial ownership) which will set out more details and further Precedents shortly.

The following table sets out some extremely high-level details in terms of what is a beneficial owner and the obligations of the specific arrangements in relation to their beneficial ownership (Regulations 5-6 and 41-44):

Type of arrangement	Who is a beneficial owner?	Obligations of arrangements
Corporate body (including LLP)	Any individual who: - exercises control over the management of the corporate body - directly/indirectly ultimately owns or controls more than 25% of the shares or voting rights (not PLCs)	On request (and within two working days), provide a relevant person with information identifying: - its name, registered number, office and principal place of business - its board or members of management body - its senior management - the law to which it is subject - its legal owners - its beneficial owners, and - its memorandum of association or other governing documents Notify any changes to beneficial ownership and date of change within two working days
Partnership	Any individual who: - directly/indirectly ultimately is entitled to or controls more than 25% share of the capital, profits or voting rights - otherwise exercises control over the management of the partnership	There do not appear to be any specific information/notification obligations on partnerships

Type of arrangement	Who is a beneficial owner?	Obligations of arrangements
Trust	Each of: - the settlor - the trustees - the beneficiaries or class of persons in whose main interest the trust is set up or operates - any individual who has control over the trust	Maintain accurate and up-to-date records of all beneficial owners equivalent to central registers information When starting a transaction/ relationship with a relevant person: - inform them it is acting as trustee - on request (and within two working days), provide information identifying all beneficial owners and any other individual referred to in any document (eg a letter of wishes) Notify any changes to beneficial ownership and date of change within two working days On request from law enforcement agency, provide beneficial ownership information If the relevant person is a trustee, they must: - retain records as per above for five years after final distribution is made - make arrangements for those records to be deleted If it is a 'taxable trust', provide specified information to the Commissioners for inclusion on a register
Foundation or other legal arrangement similar to a trust	Individuals who hold equivalent or similar positions as for beneficial ownership for trusts (above)	There do not appear to be any specific information/notification obligations on foundations or other legal arrangements similar to trusts

Enhanced due diligence

Regulation 33 says that you must apply enhanced due diligence (EDD) measures and enhanced ongoing monitoring to manage and mitigate the risks arising:

- where you have concluded there is a high risk of money laundering or terrorist financing
- in any transaction or business relationship with a person established in a country which has been identified by the EC as a high-risk third country
- where the client is a politically exposed person (PEP) or family member or close associate of a PEP, subject to exceptions—a PEP is an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official (eg heads of state, MPs, members of supreme courts, etc) and, unlike the MLR 2007, MLR 2017 ***does*** apply to domestic (UK) PEPs
- where a client has provided false or stolen documents for CDD purposes
- where the transaction(s) have no apparent economic or legal process and
  - > the transaction is complex or unusually large transactions, or
  - > where there is an unusual pattern of transactions
- in any other case which by its nature can present a higher risk of money laundering and terrorist financing

When considering whether there is a high risk of money laundering and terrorist financing and the extent of the measures to take to manage and mitigate that risk, you must take account of at least the following risk factors:

- client risk
- service, transaction or delivery channel risk
- geographical risk

The MLR 2017 set out specific elements of each risk of the risk factors which you must take account of as a minimum.

They also set out specific steps you must take in relation to PEPs, including:

- having systems to identify PEPs
- assessing the level of risk associated with that particular client
- determining what risk management systems and procedures are appropriate
- assessing the extent of the EDD to be applied
- requiring senior management approval for PEP relationships
- taking adequate measures to establish the source of wealth and source of funds involved in the business relationship
- conducting enhanced ongoing monitoring

Where EDD is required, The MLR 2017 sets out certain measures which ***must*** be taken and others which may be appropriate in certain circumstances (Regulations 33(4) and 33(5):

Measures you must take whenever EDD is required	Measures that may be appropriate depending on the requirements of the case
As far as reasonably possible, examine the background and purpose of the transaction. Increase the degree and nature of ongoing monitoring to determine whether the transaction or relationship appears to be suspicious.	Seek additional independent, reliable sources for verification purposes. Take additional measures to better understand the background, ownership and financial situation of the client and other parties Take further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship Increase the monitoring of the business relationship, including greater scrutiny of transactions.

We'll be publishing a new Practice Note (MLR 2017—client due diligence), which will set out more details, and further Precedents shortly.

Simplified due diligence

You may apply simplified due diligence (SDD) for specific transactions/business relationships which you determine present a low degree of risk of money laundering or terrorist financing, having taken into account (Regulation 36):

- your firm-wide risk assessment
- information received from the Law Society, and
- the following risk factors (which are significantly expanded on in the MLR 2017):
  - > client risk
  - > service, transaction or delivery channel risk
  - > geographical risk

Applying SDD does not mean you escape CDD measures entirely. You must still identify and verify the identity of your client, but you may adjust the extent of the measures you take, and you must still carry out sufficient ongoing monitoring to enable you to detect any unusual or suspicious transactions.

We'll be publishing a new Practice Note (MLR 2017—client due diligence), which will set out more details, and further Precedents shortly.

Regular due diligence

Regular due diligence (RDD) applies where EDD and SDD do not.

Timing

You must verify the identity of your client (and any beneficial owner) before you establish a business relationship or carry out a transaction (Regulations 30-31).

If it is necessary so as not to interrupt the normal conduct of business, and there is little risk of money laundering or terrorist financing, you can complete the verification process during the establishment of the business relationship so long as it is completed as soon as practicable after contact is first established.

Where you are unable to apply CDD you must:

- not carry out any transaction through a bank account with the client or on their behalf
- not establish a business relationship or carry out a transaction otherwise than through a bank account
- terminate any existing business relationship with the client
- consider whether you need to submit a suspicious activity report

This does not apply where you are in the course of ascertaining the legal position for a client or defending or representing that client in legal proceedings, including giving advice on the institution or avoidance of proceedings. It also does not apply to an insolvency practitioner who has been appointed by the court as administrator or liquidator of a company, where they've taken all reasonable steps to apply CDD and their resignation would be prejudicial to the interests of the creditors of the company.

Reliance on third parties

You may rely on a third party to apply CDD measures but you remain liable for any failure in applying those measures (Regulation 38).

In order to do so you must:

- obtain from the third party all the information needed to satisfy CDD requirements
- enter into a written arrangement with the third party which:
  - > allow you to obtain immediately on request (or at the latest within two working days) copies of any CDD documentation
  - > requires the third party to retain copies of those documents

This is a new requirement introduced by MLR 2017. We'll shortly be publishing a related Precedent (Third party reliance agreement).

MLR 2017 is very specific about who you can and cannot rely on:

Can rely	Cannot rely
Another relevant person who is subject to the MLR 2017 A person who carries on business in another EEA state who is: - subject to requirements in national legislation implementing 4MLD, and - supervised for compliance with the requirements laid down in 4MLD A person who carries on business in a third country who is: - subject to requirements in relation to CDD and record keeping which are equivalent to those required by 4MLD, and - supervised for compliance with those requirements in a manner which is equivalent to that in required by 4MLD Organisations whose members are any of the above Members of the same group as you, subject to additional requirements.	A third party established in a country which has been identified by the EC as a high-risk country, unless the third party is a branch or majority owned subsidiary of a party established in an EEA state

Where you are relied on by another relevant person you must, if requested by that other person and within agreed time limits (or, at the latest, within two working days):

- make available any information about your client (and any beneficial owner) which you obtained when applying CDD measures, and
- forward copies of any of those relevant documents

The MLR 2017 do not prevent you from applying CDD measures through an agent or outsourcing provider.

We'll be publishing a new Practice Note (MLR 2017—reliance on third parties), which will set out more details, and further Precedents shortly.

Enforcement, offences and penalties

MLR 2017 impose a duty on supervisory authorities to effectively monitor relevant persons and take necessary steps to ensure compliance by those they regulate, including taking appropriate measures to review the risk assessments carried out by relevant persons (Regulation 45).

Like its predecessor, the MLR 2017 provide for both civil penalties and criminal offences and penalties (Regulations 73-89 and Schedule 6).

Fines and 'naming and shaming' are both available civil penalties under MLR 2017.

In terms of criminal offences:

- it is an offence to contravene a relevant requirement of the MLR 2017, these are set out in Schedule 6 and include:
  - > risk assessment
  - > policies and procedures
  - > appointing a Nominated Officer
  - > training
  - > CDD
  - > reliance
  - > record keeping
  - > data protection
  - > beneficial ownership obligations
- there's a maximum penalty of two years imprisonment, a fine or both
- a person is not guilty of an offence if they can show they took all reasonable steps and exercised all due diligence to avoid committing the offence
- courts must have regard to whether the person followed guidance issued by a supervisory body or any other appropriate body
- a person convicted of an offence under the MLR 2017 will not also be liable to a civil penalty

There are also offences of prejudicing an investigation, making false or misleading statements, and making unlawful disclosures.

Criminal proceedings can only be brought against a relevant person. Where the relevant person is a firm, and the offence was committed with the consent or the connivance of a member of an LLP, director of a company, or the partner in a partnership, or is attributable to the lack of supervision or control or neglect on their part, the individual member, director or partner can also be prosecuted along with the firm.

Further information will be available shortly in our forthcoming Practice Note: MLR 2017—enforcement, offences and penalties.

Lexis®PSL Practice Compliance

This guide is a practice note taken from Lexis®PSL Practice Compliance. Lexis®PSL Practice Compliance is an online service designed to make risk and compliance easier to manage, whatever the size of your firm.

It comes with everything you need to get your compliance house in order and keep it that way. It provides you with access to an unbeatable range of practical guidance, templates, flowcharts, checklists and other time-saving tools. From the SRA to DPA, LeO, SOCA or ICO – we've got it covered.

Lexis®PSL Practice Management

LexisPSL Practice Management is the essential online toolkit for those who run the business side of law firms. Clear, concise practice notes by leading experts spell out exactly what good management looks like. A huge bank of templates, checklists and examples mean you don't have to reinvent the wheel and our email alerts keep you updated with what's happening across the legal market.

About the authors

Allison Wooddisse
Head of Lexis®PSL Practice Compliance
LexisNexis

Allison is a former partner of Shoosmiths, with extensive experience of legal management and practice compliance. She has recently completed an LLM in Corporate Governance, focusing on regulation of the legal sector and the challenges presented by the Legal Services Act.

Laura Spooner
Associate
LexisNexis

Laura is a Lexcel trained consultant and former Risk and Compliance Manager at Collyer Bristow Solicitors LLP, an international City firm, with extensive experience of legal management and practice compliance.

Emma Dickin
Associate
LexisNexis

Emma has worked at LexisNexis for a number of years and is an expert in legal training. She is a qualified lawyer who, prior to her career at LexisNexis, worked as a legal assistant for British American Tobacco before joining a specialist property law firm.

Catherine Innes
Associate
LexisNexis

Catherine joined LexisNexis in July 2016. She is an experienced professional support lawyer and former Director of Compliance at Trowers & Hamlins LLP where she worked closely with the COLP, COFA and management team. Prior to joining Trowers & Hamlins, Catherine worked as a Corporate solicitor at CMS Cameron McKenna and Eversheds, working mainly on private company sales and purchases, joint ventures and general company law advice.