Draft Fourth EU Money Laundering Directive – an analysis

A white paper from GB Group plc

December 2014

GBGroup
USING IDENTITY INTELLIGENTLY

Executive summary

1. The risks for businesses of being involved in money laundering or failing to comply with anti money laundering (AML) compliance obligations are significant, both financially and reputationally. Whilst businesses will balance compliance costs with commercial realities in challenging economic times, they may be forgiven for wondering whether the current AML regime is effective.
2. The European Commission's (EC) view is that more work is needed. The draft Fourth European Union (EU) Money Laundering Directive was published on 5 February 2013.
3. The draft Directive has now been considered by the relevant Committees and the European Parliament and the trilogue[1] negotiations commenced in November 2014. Those negotiations will take place over the next few months with a final version expected by the end of Q1 2015, at the latest.
4. The EC propose a more risk-based regime, greater consistency of rules across the Internal Market (with the aim of simplifying cross-border trade (so strengthening the Internal Market)) and the implementation of the revised Financial Action Taskforce (FATF) Recommendations.
5. The need for a coherent cross-border approach, at least within Europe, is vital given the already burdensome cross-border challenges faced by businesses, including the "long arm" jurisdiction requirements e.g. the USA's Foreign Account Tax Compliance Act (FATCA). Changes in regulation, whether at European level or in terms of a new regulator, whether at home or overseas, pose significant regulatory challenges for businesses.
6. The estimates of the scale of money laundering are eye-watering. In the UK, for example, turnover of serious organised crimes (mostly drug trafficking) is estimated to be around £10-15 billion each year[2] (although recent estimates in the press suggest the figure could be between £27 billion and £58 billion per year), with a significant proportion being laundered through the regulated sector.
7. Businesses already have systems[3] to report suspected money laundering, carry out AML checks (often perceived as confusing, time-consuming and costly) and even more challenging, identify (and monitor relationships with) 'politically exposed persons' (PEPs) and those on the sanctions lists[4]. The draft Directive broadens the risk-based approach, which should result in a more effective and risk-focused regime and proposes;
    - Tax crimes as a predicate offence
    - Extension of the scope to include all gambling providers, not only casinos
    - Changes to simplified and enhanced due diligence (EDD), (EDD will be required for domestic politically exposed persons (PEPs) e.g. MPs) and potentially lowering the customer due diligence (CDD) threshold for high value dealers
    - Written risk assessments by Member States **and** by regulated entities (these should improve risk mitigation/targeting of resources)
    - Transparency of beneficial ownership
    - Increased focus on data protection issues
    - Sanctions for non-compliance (e.g. administrative financial penalties up to **twice** the amount of the benefit derived from the breach where that benefit can be determined)
    - Improvements to co-operation between Financial Intelligence Units (FIU)

[1] These are the negotiations between the Parliament, the Council and the Commission to agree a common text.
[2] HM Treasury 2007
[3] Businesses are required to prevent not to detect money laundering.
[4] It is a criminal offence to carry out a transaction with persons or entities on the sanctions list unless you have a licence from HM Treasury (Financial Sanctions Team). Similar obligations apply in other jurisdictions.

Executive summary (cont)

8. Given the greater emphasis on effectiveness both in the Directive and the Financial Action Task Force's Mutual Evaluation Review (see paragraphs 26-7), prudent businesses should be reviewing their systems and controls to ensure that they are currently compliant. This will help them to prepare for the Fourth Directive. Senior management should send strong compliance messages, be aware of the proposals in the Fourth Directive and make appropriate resources available. The money laundering reporting officer (MLRO) needs to understand the details of the current proposals (as there are elements that will not change), review the current systems and plan for the changes.

9. With the introduction of the draft Directive, AML regulatory compliance should continue to be high on the Board agenda. This paper analyses the detail of the draft Directive and assesses its impact on regulated entities, to assist with planning and implementation of the proposed changes.

Introduction

10. The fight against money laundering and terrorist financing within the EU, which started with the First EU Money Laundering Directive in 1993, continued with the publication of the proposal for a Fourth EU Money Laundering Directive[5] (draft Directive) (COM(2013) 45/3) on 5 February 2013 by the EC. A proposal for a regulation[6] on information accompanying a transfer of funds (COM(2013) 44) was also published.

11. This paper examines the likely impact of the proposals on regulated entities across the EU. The details of the changes are considered below and regulated entities should plan for changes to their processes and procedures during 2015/16.

The legislative process

12. Following the publication of the drafts, the proposals have now been considered by the relevant Committees, which have proposed various amendments, following lobbying by MEPs and interested stakeholders. The European Parliament also considered the text on 11 March 2014 and proposed amendments.

13. The informal tripartite (trilogue) negotiations started in November 2014, and may result in further changes to the text. The Directive is due to be adopted by the end of quarter 1 2015 at the latest.

The rationale

14. The aim of the draft Directive is to strengthen the Internal Market, primarily in relation to financial stability, protection of society, economic prosperity and reducing cross border complexity. The Third EU Money Laundering Directive (Third ML Directive) will be repealed. The rationale is to adopt a new legal framework to counter new threats, implement the revised FATF[7] Recommendations[8] and ensure that implementation by Member States is consistent.

15. The revised Recommendations increase the focus on the effectiveness of AML/Counter Terrorist Financing (CTF) regimes (as well as technical compliance) and on the risk-based approach.

[5] A directive sets out the outcomes that Member States must achieve but each State has the flexibility to decide how to implement the directive, which must be achieved by a deadline imposed by the European Parliament.
[6] A regulation is imposed directly on all Member States and there is no flexibility about implementation.
[7] FATF is an intergovernmental body established by the G7 in 1989 to set standards and promote effective implementation of measures to fight money laundering, terrorist financing and related threats. The FATF currently comprises 34 member jurisdictions and 2 regional organisations; Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, the EC, Finland, France, Germany, Greece, Gulf Co-operation Council, Hong Kong, Iceland, India, Ireland, Italy, Japan, Republic of Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, UK and the USA.
[8] The revised Recommendations were issued on 16 February 2012.

The rationale (cont)

16. The EC also undertook its own review of the implementation of the Third ML Directive, involving consultation with a wide range of interested parties e.g. private stakeholders, regulators, supervisory authorities and commissioned an external study by Deloitte. The Deloitte study examined in detail how the Third ML Directive had been implemented in Member States and highlighted the difficulties in implementation e.g. accessing PEP/beneficial owner information, costs of compliance and interpretation differences.

17. The EC adopted a report on the application of the Third ML Directive in April 2012 and sought comments by June 2012. The subsequent Feedback Statement in July 2012 summarised the views of the wide range of stakeholders who had expressed broad support for the proposals.

Key proposals

18. The draft Directive should ensure consistency between the EU and international approaches, consistency between national rules (but allowing flexibility in implementation) and that the rules are risk-focused and can take into account emerging risks.

19. The key draft provisions are:
    - Providers of gambling services are to be brought within the scope of the draft Directive. (**Comment** - at present, only casinos are caught by the Third ML Directive. There are proposals to include online gambling operators, although Member States **may** be able to exempt proven low risk gambling services from some or all of the Directive's requirements. Finland, France and Sweden already impose obligations on other gambling operators. Germany, Denmark and the UK only impose obligations on casinos. Norway and Iceland[9] prohibit casinos.)
    - Tax crimes to be specifically included as a main offence. (**Comment** - the intention is not to have a precise definition of tax crimes but to use the existing threshold approach, i.e. it is a serious crime if punishable by at least a maximum penalty of one year in prison. This will result in greater consistency across Member States and make it clear that tax crimes are a serious matter. Countries that already have an "all crimes" approach (which includes tax crimes), such as the UK will not be affected. Due to concerns about aggressive tax planning and avoidance, there may be further amendments.)
    - New requirements to identify, assess, understand and mitigate risks as follows;
        - Each Member State is to undertake a national risk assessment (with the possibility that supranational risk assessments be undertaken in areas to be determined)
        - Obliged (i.e. regulated) entities are to take reasonable steps (proportionate to their nature and size) to identify and assess their AML/CTF risks, taking into account a set of risk factors. The assessment will have to be documented, kept up to date and made available on request to regulators and supervisors
        - Obliged entities will be required to have policies, controls and procedures (covering certain minimum requirements) to mitigate the risks identified at EU, national and business level. The draft Directive requires account to be taken of the characteristics of small entities, so that there is a proportionate approach. Depending on the size and nature of the business, an internal audit function will be required
        - Obliged entities will have to obtain approval from senior management, for the policies and procedures, who will be required to monitor/enhance the measures taken
        - (**Comment** - these risk assessment proposals are in line with the revised FATF Recommendations. As a result, the resources of supervisors can be better targeted and concentrated on the areas of greater AML/CTF risk. In the UK, the national risk assessment should be available in early 2015. Regulated businesses are already required to undertake risk assessments. Financial institutions in most jurisdictions are likely to undertake some form of risk assessment. Designated non-financial businesses and professions (DNFBPs) e.g. casinos, real estate agents, high value dealers, accountants and lawyers in jurisdictions other than the UK may not currently undertake such risk assessments.)

[9] Iceland is a member of FATF but is not currently a member of the EU.

Key proposals (cont)

- The proposed CDD changes focus on a more nuanced and less prescriptive approach, so entities are able to take a risk-based approach. This will require changes to procedures and further training of staff (see below). The main changes are;
  - The threshold for high value dealers to apply CDD when dealing with occasional transactions in cash may be reduced from €15,000 to €7,500. (**Comment** - this goes beyond the FATF Recommendations. It is not proposed to change the €15,000 limit for occasional transactions except for high-value dealers.)
  - The removal of some of the simplified due diligence (SDD) exemptions. (**Comment** - originally all the exemptions were removed as blanket exemptions were viewed by the EC as too permissive and lenient. A number of exemptions have been reinstated. Where there is no exemption, entities may be able to apply SDD, if they are satisfied that the relationship or transaction presents a lower degree of risk. See Annex II of the Directive for examples of potentially lower risk factors.)
  - Enhanced due diligence (EDD) is to be applied to domestic PEPs e.g. MPs, judges, high ranking Armed Forces Officers and those who work in international organisations at a director/deputy director/board level. Senior management approval, source of wealth/funds and ongoing monitoring will be required for domestic PEPs. Obliged entities will also need to determine whether a beneficial owner of a customer is a PEP. (**Comment** – the definitions of PEPs, family members and persons known to be close associates are the same as for foreign PEPs. EDD is likely to be required for 18 months, rather than 12 months, after the individual leaves office. The definition of senior management is amended, sufficient seniority and knowledge of the firm's AML/CTF risks is key, rather than being a member of the board. Annex III of the Directive provides examples of potentially higher risk factors relevant for EDD.)
  - Amendments to the reliance provisions requiring the obliged entity to obtain the "necessary information" about the CDD requirements from the third party and take adequate steps to ensure relevant copies of the CDD documents are forwarded immediately on request by the third party. (**Comment** - it is likely that the changes will make the reliance provisions even less helpful than at present. However, it is not yet clear what "necessary information" means.)
- Introduction of publicly accessible, interconnected ultimate beneficial ownership registers for companies and trusts. This will require companies, legal entities and express trusts to hold and make available adequate, accurate and current information on beneficial owners (BO). (**Comment** - these proposals (which go further than the FATF Recommendations) may impose significant administrative burdens on legitimate companies, trusts etc. At the UK-chaired G8 summit in June 2013, the UK committed to a range of proposals to enhance the transparency of UK company ownership and to increase trust in UK business[10]. The G8 has supported the need for transparency of ownership by issuing an Action Plan[11]. It is hoped that the 25% threshold for identification of a BO will remain unchanged, but as there are different interpretations in different Member States about what the threshold refers to, greater clarity is needed, e.g. for holding companies and foundations. Guidance may be given by the European Supervisory Authorities to ensure greater convergence between Member States.)
- The third country equivalence provisions may be removed or amended. (**Comment** – the view is that decisions should not be made on purely geographical grounds as the CDD regime is becoming more risk-based. The list of potentially lower risk factors in Annex II includes other Member States and other third countries in certain circumstances. Obliged entities do need to consider all the risk factors in Annex II and Annex III.)

[10] "Transparency and Trust: Enhancing the transparency of UK company ownership and increasing trust in UK business" consultation which closed on 16 September 2013 (www.gov.uk/government/consultations/company-ownership-transparency-and-trust-discussion-paper). The response issued on 24 April 2014 confirms that the UK will establish a publicly accessible central registry of UK company beneficial ownership information.

[11] The G8 Action Plan Principles on Combating Misuses of Companies and Legal Arrangements (www.gov.uk/government/publications/g8-action-plan-principles-to-prevent-the-misuse-of-companies-and-legal-arrangements/g8-action-plan-principles-to-prevent-the-misuse-of-companies-and-legal-arrangements

[12] Any member of the management body of the obliged entity, who is held responsible, for the exercise of functions in institutions.

[13] This includes a company. If the company is a subsidiary of a parent undertaking, the relevant total annual turnover is that of the parent undertaking in the preceding business year.

Key proposals (cont)

- Introduce a set of minimum principles-based rules to strengthen administrative sanctions. The draft Directive contains a range of sanctions (which go further than the FATF Recommendations) that Member States should ensure are available for systematic breaches by obliged entities of the key requirements of the Directive, i.e. CDD, record-keeping, reporting and internal controls. The penalties may include;
  - public reprimands
  - orders requiring entities to desist conduct
  - withdrawal of authorisation
  - temporary bans against a responsible[12] Board member
  - fines of up to 10% of the total annual turnover of a legal person[13] in the preceding business year
  - fines for individuals of up to €5M
  - fines of up to twice the amount of the benefit derived from the breach, where that benefit can be determined
  - (**Comment** – the Deloitte study found that, whilst all Member States had implemented a national sanctioning regime, the wide range of penalties made it impossible to draw comparisons. Germany does not impose criminal sanctions but Denmark, Finland, France, Sweden and the UK do. All these States impose administrative sanctions and penalties, it appears that Norway and Iceland impose administrative but not criminal sanctions.)
- Improved cross-border co-operation between Financial Intelligence Units (FIU) (e.g. between the UK's National Crime Agency (NCA) and their counterparts)
- Introduce new rules clarifying that branches and subsidiaries based in other Member States, than the head office, apply host state AML rules and reinforce co-operation arrangements between home and host supervisors. (**Comment** – this will affect entities based in different jurisdictions, the aim is to clarify the requirements on cross border businesses and the responsibilities of AML supervisors.)
- Introduce provisions to clarify the inter-action between AML/CTF and data protection requirements. The intention is to strike a balance between allowing robust systems and controls to combat money laundering and terrorist financing and protecting the rights of data subjects. There is currently a lack of clarity about the reconciliation between AML requirements and data protection requirements. (**Comment** – the EC's data protection proposals[14] including the "right to erasure" are being considered at present. A Regulation (see footnote 5) is proposed, but there are considerable concerns about the impact on businesses.)

20. The proposed Regulation on cross border wire transfers will require financial institutions to include information about the beneficiary. It will limit the possibility for exemptions from information requirements (e.g. in relation to mobile phone fund transfers). There are specific obligations on money or value transfer service providers, in particular, a requirement to file a suspicious transaction report (STR) in any country affected by the suspicious wire transfer and make relevant information available to the FIU.

21. This paper provides regulated entities with details of the proposals as currently drafted. There may be other implications that come to light during the trilogue negotiations and there may be further changes to the drafting. Businesses should keep up to date with the proposals.

[12] Any member of the management body of the obliged entity, who is held responsible, for the exercise of functions in institutions.
[13] This includes a company. If the company is a subsidiary of a parent undertaking, the relevant total annual turnover is that of the parent undertaking in the preceding business year.
[14] COM(2012) 11 final and COM(2012) 10 final

Next steps

22. The final version of the draft Directive is due to be adopted by the European Parliament by the end of quarter 1 2015 at the latest. At that point, the implementation date will be agreed. (Member States will have to transpose the Directive into national legislation by that implementation date, usually two years after adoption.)

23. Each Member State will assess what changes are required to their laws and subject to necessary consultation, will implement those changes in accordance with their national requirements. There will be differences in implementation, for example, Germany, Denmark and the UK are likely to need to extend their requirements to include gambling operators other than casinos.

24. The businesses which are not currently regulated, e.g. gambling operators other than casinos, may need to institute systems and controls to ensure compliance. Early discussions with the relevant government departments may be beneficial, so that those departments understand the potential money laundering risks involved in different types of gaming. Those businesses that are at risk of further regulation should identify how they will plan for implementation, including allocating cost and other resources. The first stage will be to consider the current regulatory requirements, (e.g. the Money Laundering Regulations 2007 in the UK) as the new provisions strengthen and build on the existing obligations.

25. Given the timetable, other regulated businesses may take the view that no action needs to be taken until 2015/16. However, this would not be prudent. Businesses should be aware of emerging risks and regulatory changes so those can be added to the risk management process.

26. The evaluation of the revised FATF Recommendations[15] commenced in 2014[16], the procedures for the Fourth Round of Mutual Evaluations having been agreed. These place greater emphasis on the effectiveness of a country's AML controls.

27. Norway and Spain have been evaluated to date and the reports are now available on the FATF website together with the outcomes from the October plenary (which includes a revised list of high risk countries).

What should regulated businesses do next?

28. Every business should assess their systems, policies and procedures to ensure that they meet the current regulatory requirements. That assessment may include the following questions;
    - Is there a culture of compliance?
    - Does senior management lead by example?
    - Do staff understand that failure to have robust money laundering systems can cause real reputational and financial damage?
    - Is CDD a tick box exercise or a risk mitigation tool?
    - Do staff obtain information on the purpose and intended nature of the business relationship with the customer so they are clear what they are being asked to do and why?
    - Do staff know what risk factors or warning signs to look for, what to report and to whom to report?
    - Are staff kept informed about AML/CTF issues on a regular basis?
    - What monitoring systems are in place?

29. A detailed assessment of current systems, including a review of the effectiveness of the procedures will enable businesses to make any changes now to improve those systems. An independent assessment by, or advice from, an external consultant e.g. on good practice, may provide businesses with reassurance that their systems are effective or more importantly, identify areas of improvement.

[15] Evaluations by FATF and Moneyval (the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism) are undertaken to assess a country's compliance with the international standards contained in those Recommendations.
[16] According to the FATF announcement on 22 February 2013 regarding the new methodology to evaluate a country's AML laws and systems and assess their effectiveness in the fight against money laundering.

What should regulated businesses do next? (cont)

30. Once businesses have undertaken that review, they will be able to identify what is likely to be required to implement the draft Directive, advise senior management, plan the changes to procedures and decide what training for staff will be required.

Customer Due Diligence (CDD)

31. CDD tends to be the most expensive and time-consuming compliance issue, due to the impact on staff and customers. If CDD systems are not commercial and practical, as well as compliant, there may be financial implications through delay or loss of customers, a key concern in the current economic climate. In addition, the recent fines demonstrate how critical it is to have robust systems in place, even if there is no suggestion that the business has been used by money launderers. Reputations are easy to damage!

32. Issues for businesses to consider may include;
    - Are the systems manual or electronic?
    - Where is the evidence held and who can access it?
    - Is there a central customer on-boarding team and if so, how does the team liaise with the customer-facing staff?
    - Are staff checking the ID information properly to see if there are concerns about the customer or are they just filing the information?
    - Are risk assessments being undertaken for customers?
    - How are staff trained on CDD, source of funds and ongoing monitoring?
    - What EDD is being undertaken for PEPs?
    - What systems are in place for enhanced ongoing monitoring of PEPs and high-risk customers?
    - What are the monitoring systems?

33. It is all too easy to implement systems and assume they work, that staff understand, not only what is being asked of them, but why, and that the systems are still "fit for purpose". Not only has the technology improved significantly, but there are likely to have been business changes since the implementation of the Third ML Directive. Businesses should be monitoring and updating their policies and procedures regularly, but this is a timely point at which to undertake a more detailed review.

34. Robust systems and controls ultimately save time, protect the business and demonstrate both compliance and effectiveness of compliance to the regulator, as well as to senior management.

PEPs/electronic verification

35. A particular challenge is that of identifying PEPs and checking whether a customer is on the sanctions list. There is still discussion about central/government lists of PEPs, but it is not clear whether those will be forthcoming. Businesses may be checking the thousands of names on the EU/UN sanctions lists[17] manually before receiving monies from or paying monies to a customer, but that experience may mean that even if there were such a list for PEPs, it would not be practical for businesses taking on significant numbers of customers. Some businesses may identify PEPs by asking their customers, but are the systems robust enough to ensure that every customer is asked whether they are related to a PEP or whether they are a known close associate of a PEP?

36. Businesses may decide it is more prudent to use an electronic verification (e-verification) provider to check the identity of customers, as well as PEPs and those on sanctions lists. (Interestingly, the Committee on Economic and Monetary Affairs tabled an amendment at Committee stage highlighting the value of e-verification.) Businesses should consider the guidance of their regulator or supervisory body and ensure the provider will comply with the relevant regulatory requirements, in particular data protection obligations. (In the UK, FCA regulated businesses will be familiar with the Joint Money Laundering Steering Group (JMLSG) guidance and the FCA's Financial Crime guidance, parts 1 and 2. The latter highlights good and poor practice, especially in relation to PEPs and sanctions.)

[17] Failure to comply with sanctions legislation in the UK is a criminal offence. The rules on penalties applicable to infringements of the EU sanctions regimes are laid out in the Member States' national laws.

What should regulated businesses do next? (cont)

37. E-verification can link a customer to both current and previous circumstances using a range of positive information sources, access to negative information sources, such as databases on identity fraud and deceased persons and access to a wide range of “alert” data sources. It is important that the provider has transparent processes so the business knows what checks are carried out, the results of those checks and the degree of certainty they provide on the identity of the customer.

38. The provider should be able to explain the scoring system, have high match rates and accuracy rates, as well as mechanisms in place to reduce the risk of false positives. If a customer does fail the check, how easy will it be to re-verify ID and will there be any additional cost? The provider needs to be able to explain from which data sources the information is obtained and provide details about whether those sources are robust. The provider’s system needs to allow a business to capture and store the information used to verify identity. A business will also require reassurance about registration with the Information Commissioner and the extent of the security of the hosting. For example, is the provider accredited with ISO:270001 and PCI:DSSv2 (Payment Card Industry Data Security Standard version 2)?

39. With increasing globalisation, most businesses will wish to use a provider that has access to a wide range of international data sources, so that they are able to check the identity of customers who hold non-UK documents.

40. E-verification confirms that an individual exists, it does not confirm that your customer is that person. Businesses should consider the risk implications and be alert to any indicators that the customer is not who they say they are. Businesses may wish to seek additional CDD material to mitigate that risk. There may be circumstances in which the business decides that e-verification is not appropriate, but it may still be an indicator of a person’s identity and at the very least provide reassurance on the PEP/sanction challenge.

41. Businesses also need to ensure that systems are in place (and are working) for senior management to approve a business relationship with a PEP and for ongoing monitoring. Do staff understand what they need to do in relation to PEPs? What information is obtained about source of wealth, as well as source of funds? Is that information consistent with the customer’s risk profile?

42. Having reviewed the current PEP procedures, a business can decide what changes (if any) are required to ensure compliance, both at present and once the draft Directive is implemented. Documenting the issues will help to show both the regulator and senior management the rationale for any changes (and the likely costs/time).

43. Whether a business decides to implement a new PEP system or simply improve the existing system, it does need to be aware of the proposed EU changes, so that any systems implemented will be “fit for purpose” in the future[18]. Businesses should ask e-verification providers what changes they will be making to provide accurate and up to date information about domestic PEPs and those working in international organisations. In particular, businesses will want to know how false positives can be minimised.

44. There are a number of aspects to consider in implementing/updating an e-verification system and external advice may assist in ensuring that any system is effective, relevant and integrated with existing systems.

Risk assessments

45. The draft Directive reinforces the existing approach to risk assessments both at business and customer level. However, the difference is that there is more detail on what risks to take into account and the requirements are formalised, as written assessments must be documented, kept up to date and made available to regulators on request.

[18] For example, all businesses will have to undertake enhanced due diligence on domestic PEPs.

What should regulated businesses do next? (cont)

46. Prudent and well-managed businesses will be identifying, managing and mitigating their risks at present. However, they should review whether they are taking appropriate and proportionate steps to identify their risks, bearing in mind the following risk factors (see Article 8 of the draft Directive);
    - Customers
    - Countries or geographic areas
    - Products
    - Services
    - Transactions
    - Delivery channels
47. Businesses that have not assessed the risks facing their business should do so now in preparation for the draft Directive. They can then target resources to manage those risks. (It is worth noting that the Committee for Economic and Monetary Affairs has also tabled an amendment that not only should Member States ensure that businesses comply with the relevant regulatory requirements, but also have systems in place that actually minimise the risks of money laundering in those businesses.)
48. Having identified the risks, businesses need to ensure that their policies and procedures mitigate those risks. The policies and procedures referred to in article 8 are likely to reflect or be similar to the obligations in national legislation, i.e. CDD, reporting, record-keeping and internal control. However, the current proposals also include compliance management (including when appropriate to the size and nature of the business, the appointment of a compliance officer at management level) and employee screening (which does not currently appear in the UK legislation). In addition, (again when appropriate to size and nature), businesses should have an independent audit function to test the policies and procedures. Businesses will also have to obtain approval from senior management for the policies and procedures who must monitor and where appropriate, enhance the measures taken.
49. Although article 8 focuses on risks for the business, businesses still need to risk assess customers and the business relationship. Article 11 requires businesses to 'assess and, as appropriate, obtain information about the purpose and intended nature of the business relationship'. The introduction of the word "assess" changes the emphasis from the existing provision, which is merely to obtain information. Businesses are likely to review how they assess not only the customer risk, but also the transaction or matter risk.
50. Annex 1 sets out a non-exhaustive list of risk variables to use when determining the extent to which CDD measures are applied:
    - The purpose of an account or relationship
    - The level of assets to be deposited by the customer or the size of transactions undertaken
    - The regularity or duration of the business relationship
51. Businesses are reminded in recital 19 of the draft Directive that risk itself is variable in nature and the variables either on their own, or in combination, may increase or decrease the potential risk posed, thus having an impact on the appropriate level of preventative measures. The new proposals should enable businesses to target their resources (and costs) more effectively.

Training

52. The training provisions in the draft Directive are broadly the same as under the Third ML Directive except there is now a proportionality element and relevant employees should be made aware of the relevant data protection requirements, as well as the AML provisions.
53. Once businesses have reviewed their policies and procedures, they are likely to need to provide further training to remind staff of their obligations and how to comply. Businesses should review not only what training they provide, but also how they provide it and how effective it is (e.g. are staff tested on their understanding of the requirements?). Good training should assist with an effective compliance culture, which results in regular queries from all parts of the business because staff keep AML at the forefront of their minds and because they understand what to look for, i.e. relevant warning signs.

What should regulated businesses do next? (cont)

54. Ensuring that compliance/AML training is effective is a real challenge and one that prudent businesses would/should be reviewing without the impetus of the draft Directive. In looking forward to implementation of new procedures, businesses will consider what training to give staff so they understand the changes in procedure, for example, dealing with domestic PEPs, potential low risk factors, potential high risk factors and the consequences of the removal of the third party equivalence provisions. The timing and details of the training also need to be considered, usually with the help of the training function in the business.

Uncertainty

55. There are still a number of unknowns and further amendments may be made to the draft Directive. Certainly, while previous Directives were being debated, MEPs were lobbied and amendments drafted, some of which were accepted by the European Parliament. It is likely that there will be changes to the current proposals.

56. The issues about transparency of beneficial ownership, both for companies and trusts continue to be a major source of discussion amongst Member States and further negotiations will take place during trilogue. The current proposals will require companies and trusts to hold adequate, accurate, current and up to date information about the entity **and** the beneficial owners, which will have to be transmitted to a publicly accessible central register. There is considerable concern about the impact of this provision in the UK because of the widespread use of trusts, unlike in other jurisdictions.

57. The formal response by the UK's Department of Business, Innovation and Skills to their consultation (see paragraph 19) was issued in April 2014 and confirms that there will be a central registry of beneficial owners that is publicly accessible. Although there are detailed requirements for companies to hold and provide information, there is currently no equivalent provision for trusts except where a qualifying beneficial interest in a company is held through a trust. There are a number of other proposals, including the prohibition of new bearer shares and a requirement that existing bearer shares are converted to registered shares over a period of time.

58. There may be further changes to the proposed data protection requirements[19] in the draft Directive and it remains to be seen whether the recent amendments to reintroduce a number of the SDD exemptions survive the trilogue negotiations.

59. Businesses are advised to stay up to date with the proposals so they can lobby their regulatory/supervisory body if changes are proposed that will have a detrimental effect, e.g. financially or on customers. This will also enable businesses to update their plans and ensure that they are prepared for the changes.

UK position

60. Once the draft Directive is adopted, HM Treasury will issue its consultation on the proposed changes, particularly to the Money Laundering Regulations. The usual consultation period is 3 months and draft legislation is anticipated in 2015. The likelihood is that the legislation will not then come into effect until the first half of 2016. Further information on the timescale will be provided as it becomes available.

Other EU jurisdictions

61. The position for other European jurisdictions may be different and those operating in other Member States are advised to keep up to date with developments in their jurisdiction. The position regarding FATF evaluations will be kept under review as that may result in earlier implementation in some jurisdictions.

[19] There continues to be debate about the separate data protection proposals and the outcome of those debates may affect the draft Directive.

Summary

62. The provisions of the draft Directive build on the existing requirements and are unlikely to require as many changes to policies and procedures as were necessary to implement the Third ML Directive. However, given the emphasis on effectiveness of AML controls, businesses should review their current systems to ensure that they are working and make appropriate changes now.

63. The main areas to review are CDD systems (including how PEPs are being identified) and how risk is assessed, at business level, customer level and transaction level. The business can then build on that review to implement the changes required by the draft Directive. However robust the systems are, they will not be effective if staff do not use them properly, either because they do not understand them or because there are insufficient incentives for compliance. Senior management has to lead by example, endorsing difficult decisions and making it clear that compliance matters, so that there is an effective compliance culture.

64. Whilst the process will take time and there will almost certainly be changes to the wording, there will be a Fourth ML Directive. There will be changes to the legislation in each Member State, so starting to prepare now is not a waste of time. Taking the time to do so will reduce the amount of work required in 2015/16 and will ensure that risks are properly managed and mitigated. The benefit for regulated businesses is that they can then target their resources. They can also ensure that their compliance costs are properly managed and demonstrate to their regulator that their systems are effective in the fight against money laundering and terrorist financing, for the ultimate benefit of society.

About the author

Alison Matthews was voted Anti Money Laundering Adviser 2014 (UK) in the Finance Monthly Awards 2014 and Money Laundering Advisor 2014 (UK) in the ACQ5 Global Awards 2014. She has advised on money laundering for over 20 years, (including 7 years in Professional Ethics at the Law Society), was an MLRO for a top 20 national law firm for over 10 years and chaired the Law Society's Money Laundering Taskforce having been an inaugural member. She lobbied on the Second and Third Directives, her AML Toolkit is published by the Law Society and she lectures for all the UK Law Societies.

Bibliography

1. Directive 2005/60/EC (Third ML Directive) and Directive 2006/70/EC (Implementing measures for PEPs, SDD etc)
2. European Commission – final study on the Application of the Ant-Money Laundering Directive (Deloitte Study) – January 24 2011
3. FATF revised Recommendations – February 2012
4. Report from the Commission to the European Parliament and the Council of 11 April 2012 on the Third AML Directive COM(2012) 168 final
5. FATF Annual Report 2012 – April 2012
6. Feedback Statement - Summary of comments on the report from the Commission July 2012
7. Proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Draft Fourth Money Laundering Directive) - COM(2013) 45/3 – February 2013
8. Proposal for a Regulation on information accompanying transfers of funds COM(2013) 44 final – February 2013
9. Commission Staff Working Document Executive Summary of the Impact Assessment SWD(2013) 21 final – February 2013
10. Commission Staff Working Document Impact Assessment SWD(2013) 21 final – February 2013
11. Speech by Martin Frohn, European Commission at the Law Society's Financial Crime Symposium on 22 March 2013
12. Speech by John Thompson, Home Office at the Law Society's Financial Crime Symposium on 22 March 2013
13. www.fatf-gafi.org
14. www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0025(COD)
15. www.gov.uk/government/consultations/company-ownership-transparency-and-trust-discussion-paper
16. www.gov.uk/government/publications/g8-action-plan-principles-to-prevent-the-misuse-of-companies-and-legal-arrangements/g8-action-plan-principles-to-prevent-the-misuse-of-companies-and-legal-arrangements
17. www.gov.uk/government/uploads/system/uploads/attachment_data/file/304297/bis-14-672-transparency-and-trust-consultation-response.pdf
18. Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation) – COM (2012) 11 final
19. Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data – COM (2012) 010 final
20. www.fca.org.uk
21. www.coe.int/t/dghl/monitoring/moneyval
22. www.gov.uk/government/organisations/hm-treasury/series/financial-sanctions-regime-specific-consolidated-lists-and-releases
23. www.jmlsg.org.uk
24. http://fshandbook.info/FS/html/FCA/FC