Client Update
Fourth Anti-Money Laundering Directive Comes Into Force

LONDON
Karolos Seeger
kseeger@debevoise.com

Matthew Howard Getz
mgetz@debevoise.com

Alex Parker
aparker@debevoise.com

Ceri Chave
cchave@debevoise.com

OVERVIEW

On 26 June 2015, the Fourth European Union Anti-Money Laundering Directive[1] (the "Directive") came into force. Member States will have until 26 June 2017 to implement the Directive into national law.

The Directive implements a risk-based legal framework that aims to counter new threats and achieve consistency across all Member States. It replaces the Third Anti-Money Laundering Directive (2005/60/EC) (the "Third Directive"), which was implemented in the UK by way of the Money Laundering Regulations 2007 (SI 2007/2157), which came into force on 15 December 2007. Among other things, the Directive focuses on terrorist financing and imposing heightened customer identification and verification requirements.

The Directive and the Proceeds of Crime Act 2002 together constitute the UK's primary anti-money laundering legislation. The principal stated objective of the Directive is to prevent the European Union's ("EU") financial system from being used for money laundering and terrorist financing purposes. It also focuses on the promotion of financial stability within the EU internal market by protecting the proper functioning and integrity of its financial systems and economic prosperity, as well as reducing regulatory cross-border complexities.

WHO IS AFFECTED?

The Directive primarily applies to the financial sector including banks, trust or company service providers, lawyers and accountants. Its scope also encompasses all dealers in goods making or receiving cash payments in excess of EUR 10,000,[2]

1 Directive (EU) 2015/849 of the European Parliament and of the Council.

2 This represents a reduction from the current level of EUR 15,000 under the Third Directive.

regardless of whether payment is made in one or more linked transactions. Such businesses are referred to as obliged or regulated entities.

SUMMARY OF MAIN CHANGES

The Directive has introduced a number of important changes, which are examined in closer detail below. In short, they are:

- All countries will need to introduce an Ultimate Beneficial Owner ("UBO") register (Articles 30 – 31) – the UK has already made some legislative changes towards this;
- Greater responsibilities will be placed on senior managers (Article 8);
- Sanctions for non-compliance will increase significantly for both individuals and firms (Articles 58 – 62);
- Implementation of a risk assessment and Senior Management regime (Articles 6 – 8);
- Simplified Due Diligence ("SDD") will be made more complex (Articles 15 – 17); and
- Enhanced Due Diligence ("EDD") will also apply to domestic Politically Exposed Persons ("PEPs") (Articles 18 – 24).

KEY CHANGES: OVERVIEW

Ultimate Beneficial Owner Register

The Directive introduces new measures to provide enhanced clarity and accessibility of UBO information by introducing a requirement, at national level, for publicly accessible, interconnected UBO registers for companies. The purpose of these provisions is to increase transparency by requiring companies to hold information about their beneficial ownership, and to make this information available to third parties via a public register.

UK Headstart

Following the UK government's introduction in March 2015 of a public register of "persons with significant control" over companies under the Small Business, Enterprise and Employment Act 2015 (the "Act"), UK companies are already required to file information on "significant controllers" with Companies House. In the case of an individual, that individual's name, month and year of birth, nationality and service address will be publicly available, together with details of the interest concerned. Residential addresses will be available from Companies

House (along with the full date of birth) only to certain public authorities, such as for law enforcement purposes. Such information must be updated annually.

The Directive: Key Provisions

The Directive goes further than the Act, insofar as it will require companies and other legal entities to hold and make available "adequate, accurate and current" information on their beneficial owners to competent authorities and obliged entities, as well as to others, such as investigative journalists and non-governmental organizations, who can demonstrate a "legitimate interest" in gaining access to the information. It remains to be seen how broadly the meaning of "legitimate interest" will be interpreted by the court.

These provisions, which aim to achieve one of the EU's core objectives of making it more difficult to cover up money laundering activity, will impose significant administrative burdens on companies.

Definition of a "Beneficial Owner" under the Directive

The definition of "beneficial owner" from the Third Directive has been retained, but revised clarification is given as to how such persons are to be identified: "*a percentage of 25% plus one share, which shall be evidence of ownership or control through shareholding and applies to every level of direct and indirect ownership.*"

If there is any doubt that the person(s) identified above are beneficial owner(s), the Directive states that "*the natural person(s) who exercises control over the management of a legal entity through other means will be deemed the beneficial owner.*" Crucially, if it is still not possible to identify the beneficial owner, the Directive introduces a third strand: "*the natural person(s) who hold the position of senior managing official(s)*" will be deemed to be the UBO.

Trusts are not required to provide information on beneficiaries as part of a public register, although information on the settlor, the trustee, the protector (if any), the beneficiaries and any other natural person exercising effective control over the trust must be collected by trustees and may be accessed by competent authorities and financial intelligence units.

The new regime potentially gives rise to a tension with data protection laws. The nature of the information available, such as an individual's name, date of birth, nationality, residency and details on ownership, could lead to inappropriate access to and use of personal information. The courts may be called upon to consider the extent to which anti-money laundering considerations trump an individual's right to privacy.

Senior Management Responsibility

Obliged entities will need to obtain approval from their senior management for the "*policies, controls and procedures that they put in place and to monitor and enhance the measures taken, where appropriate*". Senior management is defined in the Directive as "*an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors*." The language of the Directive thus provides a strong indication that it is preferable to entrust this task to someone at board level.

Increased Sanctions for Non-Compliance

The Directive contains a range of sanctions that Member States should make available for systematic breaches by obliged entities of the key Directive requirements, such as customer due diligence, record-keeping, suspicious-transaction reporting and internal controls. In relation to financial institutions, the penalties may include public reprimands, withdrawal of authorization, fines of up to 10% of the total annual turnover of a legal person[3] in the preceding business year, fines for individuals of up to EUR 5 million, or fines of up to twice the amount of the benefit derived from the breach, where that benefit can be determined.

It is, therefore, vital that businesses have robust procedures, systems and controls and resources in place to ensure compliance.

New Requirement of Written Risk Assessments

By 26 June 2017 and pursuant to the Directive, the European Commission must produce a report identifying, analysing and evaluating the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. The opinion would be made available to assist Member States and obliged entities to identify, manage and mitigate the risk of money laundering and terrorist financing.

Article 8 of the Directive requires obliged entities to "*take appropriate steps to identify and assess their money laundering and terrorist financing risks taking into account risk factors including customers, countries or geographic areas, products, services, transactions or delivery channels. These steps shall be proportionate to the nature and size of the obliged entities*." Such risk assessments will need to be

[3] 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.

documented, kept up-to-date and made available to the relevant competent authorities and self-regulatory bodies concerned.

Obliged entities are to ensure that they have policies, controls and procedures in place to mitigate and manage effectively the risks of money laundering and terrorist financing. Such policies include model risk management practices, customer due diligence, reporting, record-keeping, compliance management and employee screening.

Simplified Due Diligence will be Individually Assessed

The Directive has removed the automatic entitlement to apply SDD when obliged entities deal with specified customers and products.

Under Article 15 of the Directive, however, entities may be able to conduct SDD if they are satisfied that the relationship or transaction presents a lower degree of risk.

Potentially relevant risk factors, as set out in Annex II of the Directive, include:

- Customer risk factors, such as listed public companies subject to disclosure requirements, public administrations or enterprises.
- Product, service, transaction or delivery channel risk factors, such as life insurance policies with a low premium, financial products or services that appropriately define and limit services to certain types of customers and products, where the risks of money laundering and terrorist financing are managed by other factors, such as purse limits or transparency of ownership (e.g. certain types of electronic money).
- Geographical risk factors, such as other EU Member States, third countries with effective anti-money laundering systems or third countries with a low level of corruption or other criminal activity.

Article 17 of the Directive states that guidelines on the risk factors will be issued to competent authorities, credit institutions and financial institutions.

If properly adopted, the risk-based approach should enable regulated entities to expend less resources by simplifying procedures for low-risk clients and businesses, allowing for regulated entities to focus their resources on the highest risks, such as transactions involving high risk jurisdictions or where the transaction poses particular risks.

Broadening the Scope of Enhanced Due Diligence

Obliged entities in Member States are now required to undertake EDD when dealing with companies in designated "high-risk" countries, in order to both manage and mitigate such risks. This includes examining "*the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose*". When assessing the risks of money laundering and terrorist financing, Member States and obliged entities are required to take into account, at a minimum, the factors of potentially higher-risk situations as set out in Annex III of the Directive. These include:

- Customer risk factors, such as whether the business relationship is conducted in unusual circumstances, whether the customers are resident in geographical areas of higher risk, legal persons or arrangements that are personal asset-holding vehicles, businesses that are cash-intensive and the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.
- Product, service, transaction or delivery channel risk factors, such as private banking, products or transactions that might favour anonymity, non-face-to-face business relationships or transactions, without certain safeguards such as electronic signatures, payment received from unknown or unassociated third parties or new products and new business practices.
- Geographical risk factors, such as countries without effective anti-money laundering or counter-terrorist financing systems, countries identified by credible sources as having significant levels of corruption or other criminal activity, countries subject to sanctions, embargos or similar measures issued by, for example, the EU or the United Nations, or countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

Where branches or majority owned subsidiaries of EU obliged entities which are located in high-risk third countries fully comply with group-wide anti-money laundering procedures, EDD will not be required. Nevertheless, an obliged entity must ensure that those cases are handled using a risk-based approach, in line with the SDD procedure.

Politically Exposed Persons

Foreign PEPs, including senior political, military and judicial figures, and members of their close families, are already considered higher risk customers for anti-money laundering purposes. Article 20 of the Directive extends the PEP

definition to domestic PEPs, which include members of the administrative, management or supervisory bodies of state-owned enterprises, members of courts of auditors or of the boards of central banks, judges, Members of Parliament, Heads of State, heads of government, ministers and high ranking army officials.

With respect to transactions or business relationships with PEPs, obliged entities will be required to have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or beneficial owner of the customer is a PEP. If it is determined that a transaction or business relationship is with a PEP, obliged entities must obtain senior management approval for establishing or continuing business relationships with such persons, and take adequate measures to establish the source of wealth and source of funds involved in the business relationship or transaction with that PEP. The Directive requires EDD to be applied for 12 months after the individual (be it a foreign or domestic PEP) leaves office.

The emphasis on a risk-based approach under the Directive and the resulting changes to PEP provisions demonstrate that PEPs are a key anti-money laundering consideration. Consequently, businesses will need to amend their systems and controls to ensure that they can identify domestic PEPs. The policies and procedures will need to be revised so employees know what the EDD requirements are for such clients.

CONCLUDING REMARKS

Businesses should review their existing systems and controls to ensure that they are currently compliant with the existing regime, which will help prepare for the Directive, which is to be transposed into national law by 26 June 2017. In light of the fact that the provisions of the Directive build on existing requirements, it is unlikely that many changes to policies and procedures will be necessary, as was the case with the Third Directive. However, given the emphasis on the effectiveness of anti-money laundering controls, businesses should review their current systems and ensure they function correctly.

Senior management, who must play an increased role under the Directive, should send strong compliance messages to their organizations, be aware of the proposals in the Directive and make available appropriate resources. The assessment may look at whether:

- There is a culture of compliance.
- Senior management leads by example.

- Employees know what risk factors or warning signs to look for, what to report and to whom to report.
- Employees are kept regularly informed about anti-money laundering issues.
- Monitoring systems are in place.
- Employees understand the damage (reputational and financial) associated with failure to have robust money laundering systems in place.

Measures adopted solely at a national level, or even a European Union level, without taking into account international coordination and cooperation would have a limited effect on international criminality. The provisions in the Directive are intended to better equip Member States and obliged entities with preventative measures, institutional requirements, enforcement and prosecution issues and international cooperation to combat the threat of money laundering and terrorist financing.

* * *

Please do not hesitate to contact us with any questions.

August 3, 2015