EUROPEAN
COMMISSION

Strasbourg, XXX
COM(2013) 45 /3

2013/0025 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

(Text with EEA relevance)

{SWD(2013) 21}
{SWD(2013) 22}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

Grounds for and objectives of the proposal

The main objectives of the measures proposed are to strengthen the Internal Market by reducing complexity across borders, to safeguard the interests of society from criminality and terrorist acts, to safeguard the economic prosperity of the European Union by ensuring an efficient business environment, to contribute to financial stability by protecting the soundness, proper functioning and integrity of the financial system.

These objectives will be achieved by ensuring consistency between the EU approach and the international one; ensuring consistency between national rules, as well as flexibility in their implementation; ensuring that the rules are risk-focused and adjusted to address new emerging threats.

In addition, this proposal incorporates and repeals Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC[1], thus improving the comprehensibility and accessibility of the anti-money laundering (AML) legislative framework for all stakeholders.

The Commission intends to complement the current proposal by strengthening the EU's repressive response to money laundering. Consequently it is planned to propose criminal law harmonisation for this offence based on Article 83(1) of the Treaty on the Functioning of the European Union (TFEU) in 2013[2].

General context

The breaking down of barriers within the Internal Market facilitates not only the establishment or development of legitimate businesses across the EU, but may also provide increased opportunities for money laundering and terrorist financing. Criminals engaged in money laundering could therefore attempt to conceal or disguise the true nature, source or ownership of the assets in question and transform them into seemingly legitimate proceeds. Moreover, terrorist financing can be funded through both legitimate and criminal activities, as terrorist organisations engage in revenue-generating activities which in themselves may be, or at least appear to be, legitimate. Money laundering and terrorism financing create thus a high risk to the integrity, proper functioning, reputation and stability of the financial system, with potentially devastating consequences for the broader society.

European legislation has been adopted to protect the proper functioning of the financial system and of the Internal Market. However, the changing nature of money laundering and terrorist financing threats, facilitated by a constant evolution of technology and of the means at the disposal of criminals, requires a permanent adaptation of the legal framework to counter such threats.

---

1 OJ L 214, 4.8.2006, p. 29.

2 http://ec.europa.eu/governance/impact/planned_ia/docs/2013_home_006_money_laundering_en.pdf

At the EU level, Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing[3] (hereinafter referred to as the Third AMLD) sets out the framework designed to protect the soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole, against the risks of money laundering and terrorist financing. The EU rules are to a large extent based on international standards adopted by the Financial Action Task Force (FATF) and, as the Directive follows a minimum harmonisation approach, the framework is completed by rules adopted at national level.

At international level, the FATF has undertaken a fundamental review of the international standards and adopted a new set of Recommendations in February 2012.

In parallel to the international process, the European Commission has been undertaking its own review of the European framework. A revision of the Directive at this time is complementary to the revised FATF Recommendations, which in themselves represent a substantial strengthening of the anti-money laundering and combating terrorist financing framework. The Directive itself further strengthens elements of the revised Recommendations, in particular in relation to scope (by including providers of gambling services and dealers in goods with a threshold of EUR 7 500), beneficial ownership information (which is to be made available to obliged entities and competent authorities), and in the provisions on sanctions. It takes into account the necessity to increase effectiveness of AML measures by adapting the legal framework to ensure that risk assessments are carried out at the appropriate level and with the necessary degree of flexibility to allow adaptation to the different situations and actors. As a consequence of this, the Directive, while setting a high level of common standards, requires Member States, supervisory authorities and obliged entities to assess risk and take adequate mitigating measures commensurate to such risk. This results in the Directive being less detailed as regards concrete measures to be taken.

Existing provisions in this area

Various legal instruments have been adopted to ensure an effective anti-money laundering and combating terrorist financing framework at EU level. The most important ones are:

– The Third AML Directive, which covers most of the 40 FATF Recommendations and some of the 9 FATF Special Recommendations;

– Regulation (EC) No 1781/2006 of 15 November 2006 on information on the payer accompanying transfers of funds[4], which implements FATF SR VII on wire transfers;

– Regulation (EC) No 1889/2005 of 26 October 2005 on controls of cash entering or leaving the Community[5], which implements FATF SR IX on cash couriers;

– Directive 2007/64/EC of 13 December 2007 on payment services in the internal market[6] (Payment Services Directive) which, in combination with the Third AMLD, implements FATF SR VI on alternative remittance;

3 OJ L 309, 25.11.2005, p.15.
4 OJ L 345, 8.12.2006, p. 1.
5 OJ L 309, 25.11.2005, p. 9.
6 OJ L 319, 5.12.2007, p. 1.

– Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism[7] which, together with Regulation (EC) No 881/2002 of 27 May 2002[8] implementing UN Al Qai'da and Taliban sanctions, implements part of FATF SR III on freezing terrorist assets.

Consistency with other policies and objectives of the Union

The proposed adaptation of the anti-money laundering and combating terrorist financing framework is fully coherent with EU policies in other areas. In particular:

– the Stockholm Programme[9], which aims at achieving an open and secure Europe serving and protecting citizens, calls on Member States and the Commission to further develop information exchange between the FIUs, in the fight against money laundering;

– the EU's Internal Security Strategy[10] identifies the most urgent challenges to EU security in the years to come and proposes five strategic objectives and specific actions for 2011-2014 to help make the EU more secure. This includes tackling money laundering and preventing terrorism. The need to update the EU anti-money laundering and combating terrorist financing framework with a view to enhancing the transparency of legal persons and legal arrangements has been specifically recognised;

– the potential for misuse of new technologies to conceal transactions and hide identity makes it important for Member States to be aware of technological developments and simulate the use of electronic identification, electronic signature and trust services for electronic transactions, in line with Commission's proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market[11];

– in March 2012, the European Commission adopted a proposal on the freezing and confiscation of proceeds of crime in the EU[12] which seeks to ensure that Member States have in place an efficient system to freeze, manage and confiscate criminal assets, backed by the necessary institutional setup, financial and human resources;

– with respect to data protection, the proposed clarifications to the Third AMLD are fully in line with the approach set out in the Commission's recent data protection proposals[13], whereby a specific provision[14] empowers EU or national legislation to

7 OJ L 344, 28.12.2001, p. 70.
8 OJ L 139, 29.5.2002, p. 9.
9 OJ C 115, 4.5.2010, p. 1.
10 Communication from the Commission to the European Parliament and the Council "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (COM(2010)673 final).
11 COM(2012)238/2
12 Proposal for a Directive of the European Parliament and of the Council on the freezing and confiscation of proceeds of crime in the European Union (COM(2012)085 final).
13 Proposal for a Directive of the European Parliament and of the Council 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) and Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal

restrict the scope of the obligations and rights provided for in the draft regulation on a number of specified grounds, including the prevention, investigation, detection and prosecution of criminal offences;

– with respect to sanctions, the proposal to introduce a set of minimum principles-based rules to strengthen administrative sanctions is fully in line with the Commission's policy as outlined in its Communication "Reinforcing sanctioning regimes in the financial services sector"[15];

– with respect to financial inclusion, the fact that applying an overly cautious approach to anti-money laundering and combating terrorist financing safeguards might have the unintended consequence of excluding legitimate businesses and consumers from the financial system has been recognised. Work has been carried out on this issue at international level[16] to provide guidance to support countries and their financial institutions in designing anti-money laundering and combating terrorist financing measures that meet the national goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime. At EU level, the issue of financial inclusion is currently under consideration as part of the work on a Bank Accounts package;

– with respect to the cooperation with persons or authorities (including courts and administrative bodies) concerned with the assessment of, collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to taxes and any other public levy, the proposal is consistent with the approach for fighting against tax fraud and tax evasion[17] followed at international level in including a specific reference to tax crimes within the serious crimes which can be considered as predicate offences to money laundering. The enhancement of the customer due diligence procedures for AML purposes will also assist the fight against tax fraud and tax evasion.

2. RESULTS OF CONSULTATIONS WITH THE INTERESTED PARTIES AND IMPACT ASSESSMENTS

Consultation of interested parties

The Commission adopted in April 2012 a report on the application of the Third AMLD and solicited comments from all stakeholders. The report focused on a number of identified key themes (e.g. including application of a risk-based approach, extending the scope of the existing framework, adjusting the approach to customer due diligence, clarifying reporting obligations and supervisory powers, enhancing FIU co-operation etc.), which were essential for the review of the Third AMLD.

The Commission received 77 contributions from public authorities, civil society, business federations and companies in several fields (including financial services, gambling sector,

---

data and on the free movement of such data (General Data Protection Regulation) (COM(2012)011 final).

14 Article 21 of the General Data Protection Regulation.

15 COM(2010)716 final.

16 "Anti-money laundering and terrorist financing measures and Financial Inclusion", FATF, June 2011.

17 Commission Communication presenting an Action Plan to strengthen the fight against tax fraud and evasion, adopted by the Commission on 6 December 2012, COM(2012)722 final

liberal professions, real estate sector, trust and company service providers), representing a broad variety of stakeholders. An additional number of comments, position papers and contributions were received outside the consultation.

The overall results of the consultation[18] point to a general confirmation of the issues and problems highlighted by the Commission's Report, as well as broad support for the proposed alignment to the revised FATF standards and for greater clarification in certain areas (i.e. data protection and how to apply the rules in cross-border situations).

Use of expertise

Substantial efforts have been made to obtain evidence in this field and to ensure full engagement of the different stakeholders.

In particular, over the course of 2010, a study by external consultants Deloitte[19] was carried out on behalf of the Commission to look into the application of the Third AML Directive.

Impact assessment

The Commission has undertaken an Impact Assessment[20], where it analysed the potential consequences of money laundering and terrorism financing. In particular, the financial system failing to prevent money laundering and terrorist financing can lead to negative economic impacts (arising from disruptions to international capital flows, reduced investment and lower economic growth) and financial market instability (resulting from reluctance of other financial intermediaries to engage in business, loss of reputation, drop in confidence and prudential risks).

The following problem drivers were examined:

– the different application of existing EU rules across Member States, leading to reduced legal certainty;

– the inadequacies and loopholes with respect to the current EU rules;

– the inconsistency of the current rules with the recently revised international standards.

This requires the achievement of the following operational objectives:

– ensure consistency between national rules and, where appropriate, flexibility in their implementation by strengthening and clarifying current requirements;

– ensure that the rules are risk-focused and adjusted to address new emerging threats, by strengthening and clarifying current requirements;

[18] The feedback statement is available at http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm

[19] The study is available at http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm

[20] The impact assessment is available at http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm

– ensure that the EU approach is consistent with the approach followed at international level by extending the scope of application, strengthening and clarifying the current requirements.

The impact assessment concluded that the best options to improve the existing situation would be:

– *Broadening scope to cover gambling*: broaden the scope of the Directive beyond "casinos" to cover the gambling sector;

– *Thresholds for traders in goods*: reduce the scope and customer due diligence thresholds for traders in high value goods from EUR 15 000 to EUR 7 500 for cash transactions;

– *Sanctions regimes*: introduce a set of minimum principles-based rules to strengthen administrative sanctions;

– *Comparability of statistical data:* reinforce and make more precise the requirement regarding the collecting and reporting of statistical data;

– *Data protection:* introduce provisions in the Directive to clarify the interaction between anti-money laundering/combating terrorist financing and data protection requirements;

– *Inclusion of tax crimes in the scope*: include an explicit reference to tax crimes as a predicate offence;

– *Availability of beneficial owner information:* require all companies to hold information on their beneficial owners;

– *Identification of Beneficial Owner (BO):* maintain the approach which requires identification of the BO as of a 25% ownership threshold, but clarify what the "25% threshold" refers to;

– *Home and host supervisory responsibilities for AML*: introduce new rules clarifying that branches and subsidiaries situated in other Member States than the head office apply host state AML rules and reinforce cooperation arrangements between home and host supervisors;

– *Cross-border cooperation between Financial Intelligence Units (FIUs)*: introduce new requirements that would strengthen FIU powers and cooperation;

– *National Risk Assessments*: introduce a requirement for Member States to carry out a risk assessment at national level and take measures to mitigate risks;

– *Customer Due Diligence*: Member States to ensure that enhanced due diligence must be conducted in certain situations of high risk, while allowing them to permit simplified due diligence in lower risk situations;

– *Equivalence of third country regimes*: remove the "white list" process;

– *Risk-Sensitive Approach to supervision:* specific recognition in the Directive that supervision can be carried out on a risk-sensitive basis;

– *Treatment of Politically Exposed Persons (PEPs):* introduce new requirements for domestic PEPs/PEPs working in international organisations, with risk-sensitive measures to be applied.

In addition, the impact assessment analysed the impact of the legislative proposals on Fundamental Rights. In line with the Charter of Fundamental rights, the proposals seek in particular to ensure protection of personal data (Article 8 of the Charter) by clarifying the conditions under which personal data can be stored and transferred. The proposals will bring no change and therefore have no impact on the right to an effective remedy and to a fair trial (Article 47 of the Charter) which are not infringed by the Directive as confirmed by the European Court of Justice (case C-305/05). The respect for private life (Article 7), the freedom to conduct a business (Article 16) and the prohibition of discrimination (Article 21) have been duly taken into account. Finally, the proposal will indirectly help to protect the right to life (Article 2 of the Charter).

3. LEGAL ELEMENTS OF THE PROPOSAL

Legal basis

The current proposal is based on Article 114 TFEU.

Subsidiarity and proportionality

In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty on European Union, the objectives of the proposal cannot be sufficiently achieved by Member States and can therefore be better achieved at the Union level. The proposal does not go beyond what is necessary to achieve those objectives.

Recital 2 of the Third AMLD underlines the necessity of having measures at the EU level aiming at protecting the soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole, "in order to avoid Member States adopting measures to protect their financial systems which could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Community public policy, Community action in this area is necessary".

As massive flows of dirty money and terrorist financing can damage the stability and reputation of the financial sector and threaten the internal market, any measures adopted solely at national level could have adverse effects on the EU Single Market: an absence of coordinated rules across Member States aimed at protecting their financial systems could be inconsistent with the functioning of the internal market and result in fragmentation. EU action is also justified in order to maintain a level playing field across the EU – with entities in all Member States subject to a consistent set of anti-money laundering and combating terrorist financing obligations.

The Commission considers that the proposed rule changes are proportionate to the objectives. By imposing thresholds on scope and customer due diligence, the Commission has taken proportionate steps to limit the applicability of the Directive, where appropriate. In addition, the Directive allows certain of the preventative measures to be taken by SMEs to be

proportionate to the size and nature of the obliged entity. At the same time, by ensuring a tailored and flexible risk-based approach, Member States should not be constrained from adopting measures and taking actions as necessary to counter important threats they may confront at national level. These measures are better suited to a Directive than a fully harmonised Regulation, with the inclusion of processes at EU level to ensure greater coordination and the development of supranational approaches, together with further harmonisation in specific areas ensuring that EU objectives are also met. Although ensuring an effective AML/counter terrorism financing system entails some cost for obliged entities (these costs have been analysed in the Impact Assessment), the Commission considers that the benefits associated with preventing money laundering and terrorist financing will continue to outweigh the costs.

The evaluation of the new international standards will begin in the fourth quarter of 2013. Unless the Commission provides clear and early indications of the desired EU approach to their implementation, there is a risk that those EU Member States who will be evaluated first will opt for solutions which may not coincide with the proposed EU approach, thus rendering agreement of common EU rules more difficult.

Finally, with the adoption of revised international standards, commitments have been taken by the Commission as well as all EU Member States (either directly or via their membership of FATF or Moneyval) to ensure their implementation.

4. BUDGETARY IMPLICATION

The proposal has no implication for the budget of the European Union.

5. ADDITIONAL INFORMATION

Detailed explanation of the proposal

The main modifications to the Third AMLD are:

– *Extension of the scope of the Directive*: two main changes are proposed to the scope:

(a) the threshold for traders in high value goods dealing with cash payments be reduced from EUR 15 000 to EUR 7 500. Currently traders in goods are included in the scope of the Directive if they deal with cash payments of EUR 15 000 or more. After receiving information from Member States that this relatively high threshold was being exploited by criminals it is proposed to lower it to EUR 7 500. In addition, the new proposal requires traders to carry out customer due diligence when carrying out an occasional transaction of at least EUR 7 500, a reduction from the previous threshold of EUR 15 000. Both the definition and the threshold show a tightening of measures against the use of these traders for money laundering purposes across the EU;

(b) the scope of the Directive includes "providers of gambling services" (in accordance with Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the

Internal Market[21]). The current Third AMLD and the revised FATF Recommendations require that only casinos be included in the scope of anti-money laundering/combating terrorist financing legislation. Evidence in the EU suggests that this leaves other areas of gambling vulnerable to miss-use by criminals.

– *Risk-based approach:* The Directive recognises that the use of a risk-based approach is an effective way to identify and mitigate risks to the financial system and wider economic stability in the internal market area. The new measures proposed would require evidence-based measures to be implemented in three main areas, each of which would be supplemented with a minimum list of factors to be taken into consideration or guidance to be developed by the European Supervisory Authorities:

(a) Member States will be required to identify, understand and mitigate the risks facing them. This can be supplemented by risk assessment work carried out at a supra-national level (e.g. by the European Supervisory Authorities or Europol) and the results should be shared with other Member States and obliged entities. This would be the starting point for the risk-based approach, and would recognise that an EU-wide response can be informed by Member States' national experience;

(b) Obliged entities operating within the scope of the Directive would be required to identify, understand and mitigate their risks, and to document and update the assessments of risk that they undertake. This is a key element of the risk-based approach, allowing competent authorities (such as supervisors) within Member States to thoroughly review and understand the decisions made by obliged entities under their supervision. Ultimately, those adopting a risk-based approach would be fully accountable for the decisions they make;

(c) The proposal would recognise that the resources of supervisors can be used to concentrate on areas where the risks of money laundering and terrorist financing are greater. The use of a risk-based approach would mean that evidence is used to better target the risks.

– *Simplified and Enhanced Customer Due Diligence:* in the proposal, obliged entities would be required to take enhanced measures where risks are greater and may be permitted to take simplified measures where risks are demonstrated to be less. With regard to the current (Third) AMLD, the provisions on simplified due diligence were found to be overly permissive, with certain categories of client or transaction being given outright exemptions from due diligence requirements. The revised Directive would therefore tighten the rules on simplified due diligence and would not permit situations where exemptions apply. Instead, decisions on when and how to undertake simplified due diligence would have to be justified on the basis of risk, while minimum requirements of the factors to be taken into consideration would be given. In one of the situations where enhanced due diligence should always be conducted, namely for politically exposed persons, the Directive has been strengthened to include politically exposed persons who are entrusted with prominent public functions domestically, as well as those who work for international organisations.

[21] OJ L 178, 17.7.2000, p. 1.

– *Information on the beneficial owner:* the revised Directive proposes new measures in order to provide enhanced clarity and accessibility of beneficial ownership information. It requires legal persons to hold information on their own beneficial ownership. This information should be made available to both competent authorities and obliged entities. For legal arrangements, trustees are required to declare their status when becoming a customer and information on beneficial ownership is similarly required to be made available to competent authorities and obliged entities.

– *Third country equivalence:* the revised Directive will remove the provisions relating to positive "equivalence", as the customer due diligence regime is becoming more strongly risk-based and the use of exemptions on the grounds of purely geographical factors is less relevant. The current provisions of the Third AMLD require decisions to be made on whether third countries have anti-money laundering/combating terrorist financing systems that are "equivalent" to those in the EU. This information was then used to allow exemptions for certain aspects of customer due diligence.

– *Administrative sanctions:* in line with Commission policy to align administrative sanctions, the revised Directive contains a range of sanctions that Member States should ensure are available for systematic breaches of key requirements of the Directive, namely customer due diligence, record keeping, suspicious transaction reporting and internal controls.

– *Financial Intelligence Units:* the proposal would bring in the provisions of Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information and further extend and strengthen cooperation.

– *European Supervisory Authorities (ESA):* the proposal contains several areas where work by the ESA is envisaged. In particular, EBA, EIOPA and ESMA are asked to carry out an assessment and provide an opinion on the money laundering and terrorist financing risks facing the EU. In addition, the greater emphasis on the risk-based approach requires an enhanced degree of guidance for Member States and financial institutions on what factors should be taken into account when applying simplified customer due diligence and enhanced customer due diligence and when applying a risk-based approach to supervision. In addition, the ESAs have been tasked with providing regulatory technical standards for certain issues where financial institutions have to adapt their internal controls to deal with specific situations.

– *Data Protection*: the need to strike a balance between allowing robust systems and controls and preventative measures against money laundering and terrorist financing on the one hand, and protecting the rights of data subjects on the other is reflected in the proposal.

– *Transposition measures:* Due to the complexity and scope of the proposal, Member States are required to transmit a correlation table of the provisions of their national law and the Directive.

European Economic Area

The proposal is relevant for the EEA countries.

2013/0025 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the European Central Bank[2],

After consulting the European Data Protection Supervisor[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Massive flows of dirty money can damage the stability and reputation of the financial sector and threaten the single market, and terrorism shakes the very foundations of our society. In addition to the criminal law approach, a preventive effort via the financial system can produce results.

(2) The soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to channel lawful or unlawful money for terrorist purposes. In order to facilitate their criminal activities, money launderers and terrorist financers could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the integrated financial area entails, if certain coordinating measures are not adopted at Union level.

---

1 OJ C , , p. .
2 OJ C , , p. .
3 OJ C , , p. .

(3) The current proposal is the fourth Directive to deal with the threat of money laundering. Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering[4] defined money laundering in terms of drugs offences and imposed obligations solely on the financial sector. Directive 2001/97/EC of the European Parliament and of the Council of December 2001 amending Council Directive 91/308/EEC[5] extended the scope both in terms of the crimes covered and the range of professions and activities covered. In June 2003 the Financial Action Task Force (hereinafter referred to as the FATF) revised its Recommendations to cover terrorist financing, and provided more detailed requirements in relation to customer identification and verification, the situations where a higher risk of money laundering may justify enhanced measures and also situations where a reduced risk may justify less rigorous controls. These changes were reflected in Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing[6] and Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis[7].

(4) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even European Union level, without taking account of international coordination and cooperation, would have very limited effects. The measures adopted by the European Union in this field should therefore be consistent with other action undertaken in other international fora. The European Union action should continue to take particular account of the Recommendations of the FATF, which constitutes the foremost international body active in the fight against money laundering and terrorist financing. With the view to reinforce the efficacy of the fight against money laundering and terrorist financing, Directives 2005/60/EC and 2006/70/EC should be aligned with the new FATF Recommendations adopted and expanded in February 2012.

(5) Furthermore, the misuse of the financial system to channel criminal or even clean money to terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. Accordingly, the preventive measures of this Directive should cover not only the manipulation of money derived from crime but also the collection of money or property for terrorist purposes.

(6) The use of large cash payments is vulnerable to money laundering and terrorist financing. In order to increase vigilance and mitigate the risks posed by cash payments natural or legal persons trading in goods should be covered by this Directive to the extent that they make or receive cash payments of EUR 7 500 or more. Member States may decide to adopt stricter provisions including a lower threshold.

(7) Legal professionals, as defined by the Member States, should be subject to the provisions of this Directive when participating in financial or corporate transactions,

---

4 OJ L 166, 28.6.1991, p. 77.
5 OJ L 344, 28.12.2001, p. 76.
6 OJ L 309, 25.11.2005, p. 15.
7 OJ L 214, 4.8.2006, p. 29.

including providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing. There should, however, be exemptions from any obligation to report information obtained either before, during or after judicial proceedings, or in the course of ascertaining the legal position of a client. Thus, legal advice should remain subject to the obligation of professional secrecy unless the legal counsellor is taking part in money laundering or terrorist financing, the legal advice is provided for money laundering or terrorist financing purposes or the lawyer knows that the client is seeking legal advice for money laundering or terrorist financing purposes.

(8) Directly comparable services should be treated in the same manner when provided by any of the professionals covered by this Directive. In order to ensure the respect of the rights guaranteed by the Charter of Fundamental Rights of the European Union, in the case of auditors, external accountants and tax advisors, who, in some Member States, may defend or represent a client in the context of judicial proceedings or ascertain a client's legal position, the information they obtain in the performance of those tasks should not be subject to the reporting obligations in accordance with this Directive.

(9) It is important to expressly highlight that "tax crimes" related to direct and indirect taxes are included in the broad definition of "criminal activity" under this Directive in line with the revised FATF Recommendations.

(10) There is a need to identify any natural person who exercises ownership or control over a legal person. While finding a percentage shareholding will not automatically result in finding the beneficial owner, it is an evidential factor to be taken into account. Identification and verification of beneficial owners should, where relevant, extend to legal entities that own other legal entities, and should follow the chain of ownership until the natural person who exercises ownership or control of the legal person that is the customer is found.

(11) The need for accurate and up-to-date information on the beneficial owner is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure. Member States should therefore ensure that companies retain information on their beneficial ownership and make this information available to competent authorities and obliged entities. In addition, trustees should declare their status to obliged entities.

(12) This Directive should also apply to those activities of the obliged entities covered by this Directive which are performed on the internet.

(13) The use of the gambling sector to launder the proceeds of criminal activity is of concern. In order to mitigate the risks related to the sector and to provide parity amongst the providers of gambling services, an obligation for all providers of gambling services to conduct customer due diligence for single transactions of EUR 2 000 or more should be laid down. Member States should consider applying this threshold to the collection of winnings as well as wagering a stake. Providers of gambling services with physical premises (e.g. casinos and gaming houses) should ensure that customer due diligence, if it is taken at the point of entry to the premises, can be linked to the transactions conducted by the customer on those premises.

(14) The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a risk-based approach should be used. The risk-based approach is not an unduly permissive option for Member States and obliged entities. It involves the use of evidence-based decision making to better target the money laundering and terrorist financing risks facing the European Union and those operating within it.

(15) Underpinning the risk-based approach is a need for Member States to identify, understand and mitigate the money laundering and terrorist financing risks it faces. The importance of a supra-national approach to risk identification has been recognised at international level, and the European Supervisory Authority (European Banking Authority) (hereinafter 'EBA'), established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC[8]; the European Supervisory Authority (European Insurance and Occupational Pensions Authority) (hereinafter 'EIOPA'), established by Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC[9]; and the European Supervisory Authority (European Securities and Markets Authority) (hereinafter 'ESMA'), established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC[10], should be tasked with issuing an opinion on the risks affecting the financial sector.

(16) The results of risk assessments at Member State level should, where appropriate, be made available to obliged entities to enable them to identify, understand and mitigate their own risks.

(17) In order to better understand and mitigate risks at European Union level, Member States should share the results of their risk assessments with each other, the Commission and EBA, EIOPA and ESMA, where appropriate.

(18) When applying the provisions of this Directive, it is appropriate to take account of the characteristics and needs of small obliged entities which fall under its scope, and to ensure a treatment which is appropriate to the specific needs of small obliged entities, and the nature of the business.

(19) 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, such as customer due diligence measures. Thus, there are circumstances in which enhanced due diligence should be applied and others in which simplified due diligence may be appropriate.

(20) It should be recognised that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all

[8] OJ L 331, 15.12.2010, p. 12.
[9] OJ L 331, 15.12.2010, p. 48.
[10] OJ L 331, 15.12.2010, p. 84.

customers should be established, there are cases where particularly rigorous customer identification and verification procedures are required.

(21) This is particularly true of business relationships with individuals holding, or having held, important public positions, particularly those from countries where corruption is widespread. Such relationships may expose the financial sector in particular to significant reputational and legal risks. The international effort to combat corruption also justifies the need to pay special attention to such cases and to apply appropriate enhanced customer due diligence measures in respect of persons who hold or have held prominent functions domestically or abroad and senior figures in international organisations.

(22) Obtaining approval from senior management for establishing business relationships need not, in all cases, imply obtaining approval from the board of directors. Granting of such approval should be possible by someone with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to make decisions affecting its risk exposure.

(23) In order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers whose identification has been carried out elsewhere to be introduced to the obliged entities. Where an obliged entity relies on a third party, the ultimate responsibility for the customer due diligence procedure remains with the obliged entity to whom the customer is introduced. The third party, or the person that has introduced the customer, should also retain his own responsibility for compliance with the requirements in this Directive, including the requirement to report suspicious transactions and maintain records, to the extent that he has a relationship with the customer that is covered by this Directive.

(24) In the case of agency or outsourcing relationships on a contractual basis between obliged entities and external natural or legal persons not covered by this Directive, any anti money laundering and anti-terrorist financing obligations for those agents or outsourcing service providers as part of the obliged entities, may only arise from contract and not from this Directive. The responsibility for complying with this Directive should remain with the obliged entity covered hereby.

(25) All Member States have, or should, set up financial intelligence units (hereinafter referred to as FIUs) to collect and analyse the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing. Suspicious transactions should be reported to the FIUs, which should serve as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing. This should not compel Member States to change their existing reporting systems where the reporting is done through a public prosecutor or other law enforcement authorities, as long as the information is forwarded promptly and unfiltered to FIUs, allowing them to perform their tasks properly, including international cooperation with other FIUs.

(26) By way of derogation from the general prohibition on executing suspicious transactions, obliged entities may execute suspicious transactions before informing the

competent authorities, where refraining from the execution thereof is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. This, however, should be without prejudice to the international obligations accepted by the Member States to freeze without delay funds or other assets of terrorists, terrorist organisations or those who finance terrorism, in accordance with the relevant United Nations Security Council resolutions.

(27) Member States should have the possibility to designate an appropriate self-regulatory body of the professions referred to in Article 2(1)(3)(a),(b), and (d) as the authority to be informed in the first instance in place of the FIU. In line with the case law of the European Court of Human Rights, a system of first instance reporting to a self-regulatory body constitutes an important safeguard to uphold the protection of fundamental rights as concerns the reporting obligations applicable to lawyers.

(28) Where a Member State decides to make use of the exemptions provided for in Article 33(2), it may allow or require the self-regulatory body representing the persons referred to therein not to transmit to the FIU any information obtained from those persons in the circumstances referred to in that Article.

(29) There have been a number of cases of employees who report their suspicions of money laundering being subjected to threats or hostile action. Although this Directive cannot interfere with Member States' judicial procedures, this is a crucial issue for the effectiveness of the anti-money laundering and anti-terrorist financing system. Member States should be aware of this problem and should do whatever they can to protect employees from such threats or hostile action.

(30) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[11], as implemented in national law, is applicable to the processing of personal data for the purposes of this Directive.

(31) Certain aspects of the implementation of this Directive involve the collection, analysis, storage and sharing of data. The processing of personal data should be permitted in order to comply with the obligations laid down in this Directive, including carrying out of customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, sharing of information by competent authorities and sharing of information by financial institutions. The personal data collected should be limited to what is strictly necessary for the purpose of complying with the requirements of this Directive and not further processed in a way inconsistent with Directive 95/46/EC. In particular, further processing of personal data for commercial purposes should be strictly prohibited.

(32) The fight against money-laundering and terrorist financing is recognised as an important public interest ground by all Member States.

(33) This Directive is without prejudice to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, including the provisions of Framework decision 977/2008/JHA.

---

[11] OJ L 281, 23.11.1995, p. 31.

(34) The rights of access of the data subject are applicable to the personal data processed for the purpose of this Directive. However, access by the data subject to information contained in a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Limitations to this right in accordance with the rules laid down in Article 13 of Directive 95/46/EC may therefore be justified.

(35) Persons who merely convert paper documents into electronic data and are acting under a contract with a credit institution or a financial institution do not fall within the scope of this Directive, nor does any natural or legal person that provides credit or financial institutions solely with a message or other support systems for transmitting funds or with clearing and settlement systems.

(36) Money laundering and terrorist financing are international problems and the effort to combat them should be global. Where Union credit and financial institutions have branches and subsidiaries located in third countries where the legislation in this area is deficient, they should, in order to avoid the application of very different standards within the institution or group of institutions, apply Union standards or notify the competent authorities of the home Member State if application of such standards is impossible.

(37) Feedback should, where practicable, be made available to obliged entities on the usefulness and follow-up of the suspicious transactions reports they present. To make this possible, and to be able to review the effectiveness of their systems to combat money laundering and terrorist financing Member States should keep and improve the relevant statistics. To further enhance the quality and consistency of the statistical data collected at Union level, the Commission should keep track of the EU-wide situation with respect to the fight against money laundering and terrorist financing and publish regular overviews.

(38) Competent authorities should ensure that, in regard to currency exchange offices, trust and company service providers or gambling service providers, the persons who effectively direct the business of such entities and the beneficial owners of such entities are fit and proper persons. The criteria for determining whether or not a person is fit and proper should, as a minimum, reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.

(39) Taking into account the transnational character of money laundering and terrorist financing, co-ordination and co-operation between EU FIUs are extremely important. This co-operation has so far only been addressed by Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information[12]. In order to ensure better co-ordination and cooperation between FUIs, and in particular to ensure that suspicious transactions reports reach the FIU of the Member State where the report would be of most use, more detailed, further going and up-dated rules should be included in this Directive.

(40) Improving the exchange of information between FIUs within the EU is of particular importance to face the transnational character of money laundering and terrorist

[12] OJ L 271, 24.10.2000, p. 4.

financing. The use of secure facilities for the exchange of information, especially the decentralised computer network FIU.net and the techniques offered by that network should be encouraged by Member States.

(41) The importance of combating money laundering and terrorist financing should lead Member States to lay down effective, proportionate and dissuasive sanctions in national law for failure to respect the national provisions adopted pursuant to this Directive. Member States currently have a diverse range of administrative measures and sanctions for breaches of the key preventative measures. This diversity could be detrimental to the efforts put in combating money laundering and terrorist financing and the Union's response is at risk of being fragmented. This Directive should therefore include a range of administrative measures and sanctions that Member States shall have available for systematic breaches of the requirements relating to customer due diligence measures, record keeping, reporting of suspicious transactions and internal controls of obliged entities. This range should be sufficiently broad to allow Member States and competent authorities to take account of the differences between obliged entities, in particular between financial institutions and other obliged entities, as regards their size, characteristics and areas of activity. In the application of this Directive, Member States should ensure that the imposition of administrative measures and sanctions in accordance with this Directive and of criminal sanctions in accordance with national law does not breach the principle of *ne bis in idem*.

(42) Technical standards in financial services should ensure consistent harmonisation and adequate protection of depositors, investors and consumers across the Union. As bodies with highly specialised expertise, it would be efficient and appropriate to entrust EBA, EIOPA and ESMA with the elaboration of draft regulatory technical standards which do not involve policy choices, for submission to the Commission.

(43) The Commission should adopt the draft regulatory technical standards developed by EBA, EIOPA and ESMA pursuant to Article 42 of this Directive by means of delegated acts pursuant to Article 290 of the Treaty on the Functioning of the European Union and in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010, Regulation (EU) No 1094/2010 and Regulation (EU) No 1095/2010.

(44) In view of the very substantial amendments that would need to be made to Directive 2005/60/EC and Directive 2006/70/EC, they should be merged and replaced for reasons of clarity and consistency.

(45) Since the objective of this Directive, namely the protection of the financial system by means of prevention, investigation and detection of money laundering and terrorist financing, cannot be sufficiently achieved by the Member States, as individual measures adopted by Member States to protect their financial systems could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Union public policy and can therefore, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(46) This Directive respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular, the respect for private and family life, the right to protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, and the right of defence.

(47) In line with Article 21 of the EU Charter of Fundamental Rights prohibiting any discrimination based on any ground, Member States have to ensure that this Directive is implemented, as regards risk assessments in the context of customer due diligence, without discrimination.

(48) In accordance with the Joint Political Declaration of Member States and the Commission of 28 September 2011 on explanatory documents, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

SECTION 1

SCOPE AND DEFINITIONS

Article 1

1. Member States shall ensure that money laundering and terrorist financing are prohibited.

2. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:

   (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

   (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such

property is derived from criminal activity or from an act of participation in such activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

3. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

4. For the purposes of this Directive, 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism[13], as amended by Council Framework Decision 2008/919/JHA of 28 November 2008[14].

5. Knowledge, intent or purpose required as an element of the activities referred to in paragraphs 2 and 4 may be inferred from objective factual circumstances.

Article 2

1. This Directive shall apply to the following obliged entities:

(1) credit institutions;

(2) financial institutions;

(3) the following legal or natural persons acting in the exercise of their professional activities:

(a) auditors, external accountants and tax advisors;

(b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for their client concerning the:

(i) buying and selling of real property or business entities;

(ii) managing of client money, securities or other assets;

(iii) opening or management of bank, savings or securities accounts;

[13] OJ L 164, 22.6.2002, p. 3.
[14] OJ L 330, 9.12.2008, p. 21-23.

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies or similar structures;

(c) trust or company service providers not already covered under points (a) or (b);

(d) real estate agents, including letting agents;

(e) other natural or legal persons trading in goods, only to the extent that payments are made or received in cash in an amount of EUR 7 500 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked;

(f) providers of gambling services.

2. Member States may decide that legal and natural persons, who engage in a financial activity on an occasional or very limited basis where there is little risk of money laundering or terrorist financing occurring, do not fall within the scope of this Directive provided that the legal or natural person fulfils all of the following criteria:

(a) the financial activity is limited in absolute terms;

(b) the financial activity is limited on a transaction basis;

(c) the financial activity is not the main activity;

(d) the financial activity is ancillary and directly related to the main activity;

(e) the main activity is not an activity mentioned in paragraph 1, with the exception of the activity referred to in point (3)(e) of paragraph 1;

(f) the financial activity is provided only to the customers of the main activity and is not generally offered to the public.

The previous subparagraph shall not apply to the legal and natural persons engaged in the activity of money remittance within the meaning of Article 4(13) of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC[15].

3. For the purposes of point (a) of paragraph 2, Member States shall require that the total turnover of the financial activity may not exceed a threshold which must be sufficiently low. That threshold shall be established at national level, depending on the type of financial activity.

4. For the purposes of point (b) of paragraph 2, Member States shall apply a maximum threshold per customer and single transaction, whether the transaction is carried out in a single operation or in several operations which appear to be linked. That

[15] OJ L 319, 5.12.2007, p. 1.

threshold shall be established at national level, depending on the type of financial activity. It shall be sufficiently low in order to ensure that the types of transactions in question are an impractical and inefficient method for laundering money or for terrorist financing, and shall not exceed EUR 1 000.

5. For the purposes of point (c) of paragraph 2, Member States shall require that the turnover of the financial activity does not exceed 5 % of the total turnover of the legal or natural person concerned.

6. In assessing the risk of money laundering or terrorist financing occurring for the purposes of this Article, Member States shall pay special attention to any financial activity which is regarded as particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.

7. Any decision pursuant to this Article shall state the reasons on which it is based. Member States shall provide for the possibility of withdrawing that decision should circumstances change.

8. Member States shall establish risk-based monitoring activities or take any other adequate measures to ensure that the exemption granted by decisions pursuant to this Article is not abused.

Article 3

For the purposes of this Directive the following definitions shall apply:

(1) "credit institution" means a credit institution, as defined in Article 4(1) of Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions[16], including branches within the meaning of Article 4(3) of that Directive located in the European Union of credit institutions having their head offices inside or outside the European Union;

(2) "financial institution" means:

(a) an undertaking, other than a credit institution, which carries out one or more of the operations included in points 2 to 12 and points 14 and 15 of Annex I to Directive 2006/48/EC, including the activities of currency exchange offices (bureaux de change);

(b) an insurance company duly authorised in accordance with Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance[17], insofar as it carries out activities covered by that Directive;

(c) an investment firm as defined in point 1 of Article 4(1) of Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments[18];

[16] OJ L 177, 30.6.2006, p. 1.
[17] OJ L 345, 19.12.2002, p. 1.
[18] OJ L 145, 30.4.2004, p. 1.

(d) a collective investment undertaking marketing its units or shares;

(e) an insurance intermediary as defined in Article 2(5) of Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation[19], with the exception of intermediaries as mentioned in Article 2(7) of that Directive, when they act in respect of life insurance and other investment related services;

(f) branches, when located in the European Union, of financial institutions as referred to in points (a) to (e), whose head offices are inside or outside the European Union;

(3) "property" means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;

(4) "criminal activity" means any kind of criminal involvement in the commission of the following serious crimes:

(a) acts as defined in Articles 1 to 4 of Framework Decision 2002/475/JHA on combatting terrorism, as amended by Council Framework Decision 2008/919/JHA of 28 November 2008;

(b) any of the offences referred in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;

(c) the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union[20];

(d) fraud affecting the Union's financial interests, at least serious, as defined in Article 1(1) and Article 2 of the Convention on the Protection of the European Communities' Financial Interests[21];

(e) corruption;

(f) all offences, including tax crimes related to direct taxes and indirect taxes, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months;

(5) "beneficial owner" means any natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:

---

19 OJ L 9, 15.1.2003, p. 3.

20 OJ L 351, 29.12.1998, p. 1.

21 OJ C 316, 27.11.1995, p. 49.

(a) in the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Union legislation or subject to equivalent international standards.

A percentage of 25% plus one share shall be evidence of ownership or control through shareholding and applies to every level of direct and indirect ownership;

(ii) if there is any doubt that the person(s) identified in point (i) are the beneficial owner(s), the natural person(s) who exercises control over the management of a legal entity through other means;

(b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:

(i) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity; and

(ii) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity; or

(iii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates. For beneficiaries of trusts that are designated by characteristics or by class, obliged entities shall obtain sufficient information concerning the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights;

(6) "trust or company service providers" means any natural or legal person which by way of business provides any of the following services to third parties:

(a) forming companies or other legal persons;

(b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;

(d) acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement;

(e) acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with European Union legislation or subject to equivalent international standards;

(7) (a) "foreign politically exposed persons" means natural persons who are or have been entrusted with prominent public functions by a third country;

(b) "domestic politically exposed persons" means natural persons who are or who have been entrusted by a Member State with prominent public functions;

(c) "persons who are or who have been entrusted with a prominent function by an international organisation" means directors, deputy directors and members of the board or equivalent function of an international organisation;

(d) "natural persons who are or have been entrusted with prominent public functions" shall include the following:

(i) heads of State, heads of government, ministers and deputy or assistant ministers;

(ii) members of parliaments;

(iii) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

(iv) members of courts of auditors or of the boards of central banks;

(v) ambassadors, *chargés d'affaires* and high-ranking officers in the armed forces;

(vi) members of the administrative, management or supervisory bodies of State owned enterprises.

None of the categories set out in points (i) to (vi) shall be understood as covering middle ranking or more junior officials;

(e) "family members" shall include the following:

(i) the spouse;

(ii) any partner considered as equivalent to the spouse;

(iii) the children and their spouses or partners;

(iv) the parents;

(f) "persons known to be close associates" shall include the following:

(i) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in points (7)(a) to (7)(d) above;

(ii) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in points (7)(a) to (7)(d) above;

(8) "senior management" means an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to make decisions affecting its risk exposure. It need not, in all cases, involve a member of the board of directors;

(9) "business relationship" means a business, professional or commercial relationship which is connected with the professional activities of the obliged entities and which is expected, at the time when the contact is established, to have an element of duration;

(10) "gambling services" means any service which involves wagering a stake with monetary value in games of chance including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services;

(11) "group" has the meaning given to it in Article 2(12) of Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate[22].

Article 4

1. Member States shall ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the obliged entities referred to in Article 2(1), which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes.

2. Where a Member State decides to extend the provisions of this Directive to professions and to categories of undertakings other than those referred to in Article 2(1), it shall inform the Commission thereof.

Article 5

The Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing.

[22] OJ L 35, 11.2.2003, p. 1.

SECTION 2

RISK ASSESSMENT

Article 6

1. The European Banking Authority (hereinafter "EBA"), European Insurance and Occupational Pensions Authority (hereinafter "EIOPA") and European Securities and Markets Authority (hereinafter "ESMA") shall provide a joint opinion on the money laundering and terrorist financing risks affecting the internal market.

   The opinion shall be provided within 2 years from the date of entry into force of this Directive.

2. The Commission shall make the opinion available to assist Member States and obliged entities to identify, manage and mitigate the risk of money laundering and terrorist financing.

Article 7

1. Each Member State shall take appropriate steps to identify, assess, understand and mitigate the money laundering and terrorist financing risks affecting it, and keep the assessment up-to-date.

2. Each Member State shall designate an authority to co-ordinate the national response to the risks referred to in paragraph 1. The identity of that authority shall be notified to the Commission, EBA, EIOPA and ESMA and other Member States.

3. In carrying out the assessments referred to in paragraph 1, Member States may make use of the opinion referred to in Article 6(1).

4. Each Member State shall carry out the assessment referred to in paragraph 1 and:

   (a) use the assessment(s) to improve its anti-money laundering and combating terrorist financing regime, in particular by identifying any areas where obliged entities shall apply enhanced measures and, where appropriate, specifying the measures to be taken;

   (b) use the assessment(s) to assist it in the allocation and prioritisation of resources to combat money laundering and terrorist financing;

   (c) make appropriate information available to obliged entities to carry out their own money laundering and terrorist financing risk assessments.

5. Member States shall make the results of their risk assessments available to the other Member States, the Commission, and EBA, EIOPA and ESMA upon request.

Article 8

1. Member States shall ensure that obliged entities 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.

2. The assessments referred to in paragraph 1 shall be documented, kept up to date and be made available to competent authorities and self-regulatory bodies.

3. Member States shall ensure that obliged entities have policies, controls and procedures to mitigate and manage effectively the money laundering and terrorist financing risks identified at Union level, Member State level, and at the level of obliged entities. Policies, controls and procedures should be proportionate to the nature and size of those obliged entities.

4. The policies and procedures referred to in paragraph 3 shall at least include:

   (a) the development of internal policies, procedures and controls, including customer due diligence, reporting, record keeping, internal control, 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;

   (b) when appropriate with regard to the size and nature of the business, an independent audit function to test internal policies, procedures and controls referred to in point (a).

5. Member States shall require obliged entities to obtain approval from senior management for the policies and procedures they put in place, and shall monitor and enhance the measures taken, where appropriate.

CHAPTER II

CUSTOMER DUE DILIGENCE

SECTION 1

GENERAL PROVISIONS

Article 9

Member States shall prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks. Member States shall in all cases require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be made the

subject of customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.

Article 10

Member States shall ensure that obliged entities apply customer due diligence measures in the following cases:

(a) when establishing a business relationship;

(b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(c) for natural or legal persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 7 500 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(d) for providers of gambling services, when carrying out occasional transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

(f) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Article 11

1. Customer due diligence measures shall comprise:

   (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

   (b) identifying the beneficial owner and taking reasonable measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;

   (c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

   (d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

2. Member States shall ensure that obliged entities apply each of the customer due diligence requirements set out in paragraph 1, but may determine the extent of such measures on a risk-sensitive basis.

3. When assessing money laundering and terrorist financing risks, Member States shall require obliged entities to take into account at least the variables set out in Annex I.

4. Member States shall ensure that obliged entities are able to demonstrate to competent authorities or self-regulatory bodies that the measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified.

5. For life or other investment-related insurance business, Member States shall ensure that financial institutions shall, in addition to the customer due diligence measures required for the customer and the beneficial owner, conduct the following customer due diligence measures on the beneficiaries of life insurance and other investment related insurance policies, as soon as the beneficiaries are identified or designated:

   (a) for beneficiaries that are identified as specifically named natural or legal persons or legal arrangements, taking the name of the person;

   (b) for beneficiaries that are designated by characteristics or by class or by other means, obtaining sufficient information concerning those beneficiaries to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

   For both the cases referred to in points (a) and (b), the verification of the identity of the beneficiaries shall occur at the time of the payout. In case of assignment, in whole or in part, of the life or other investment related insurance to a third party, financial institutions aware of the assignment shall identify the beneficial owner at the time of the assignment to the natural or legal person or legal arrangement receiving for own benefit the value of the policy assigned.

Article 12

1. Member States shall require that the verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying-out of the transaction.

2. By way of derogation from paragraph 1, Member States may allow the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact.

3. By way of derogation from paragraphs 1 and 2, Member States may allow the opening of a bank account provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with paragraphs 1 and 2 is obtained.

4. Member States shall require that, where the institution or person concerned is unable to comply with points (a), (b) and (c) of Article 11(1), it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, and shall consider terminating the business relationship and making a suspicious transaction report to the financial intelligence unit (FIU) in accordance with Article 32 in relation to the customer.

   Member States shall not apply the previous subparagraph to, notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such exemption relates to ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings.

5. Member States shall require that obliged entities apply the customer due diligence procedures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, including at times when the relevant circumstances of a customer change.

SECTION 2

SIMPLIFIED CUSTOMER DUE DILIGENCE

Article 13

1. Where a Member State or an obliged entity identifies areas of lower risk, that Member State may allow obliged entities to apply simplified customer due diligence measures.

2. Before applying simplified customer due diligence measures obliged entities shall ascertain that the customer relationship or transaction presents a lower degree of risk.

3. Member States shall ensure that obliged entities carry out sufficient monitoring of the transaction or business relationship to enable the detection of unusual or suspicious transactions.

Article 14

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, Member States and obliged entities shall take into account at least the factors of potentially lower risk situations set out in Annex II.

Article 15

EBA, EIOPA and ESMA shall issue guidelines addressed to competent authorities and the obliged entities referred to in Article 2(1)(1) and (2) in accordance with Article 16 of

Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010, on the risk factors to be taken into consideration and/or the measures to be taken in situations where simplified due diligence measures are appropriate. Specific account should be taken of the nature and size of the business, and where appropriate and proportionate, specific measures should be foreseen. These guidelines shall be issued within 2 years of the date of entry into force of this Directive.

SECTION 3

ENHANCED CUSTOMER DUE DILIGENCE

Article 16

1. In cases identified in Articles 17 to 23 of this Directive and in other cases of higher risks that are identified by Member States or obliged entities, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.

2. Member States shall require obliged entities to examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. In particular, they shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

3. When assessing the money laundering and terrorist financing risks, Member States and obliged entities shall take into account at least the factors of potentially higher-risk situations set out in Annex III.

4. EBA, EIOPA and ESMA shall issue guidelines addressed to competent authorities and the obliged entities referred to Article 2(1)(1) and (2) in accordance with Article 16 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010 on the risk factors to be taken into consideration and/or the measures to be taken in situations where enhanced due diligence measures need to be applied. Those guidelines shall be issued within 2 years of the date of entry into force of this Directive.

Article 17

In respect of cross-frontier correspondent banking relationships with respondent institutions from third countries, Member States shall, in addition to the customer due diligence measures as set out in Article 11, require their credit institutions to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;

(b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls;

(c) obtain approval from senior management before establishing new correspondent banking relationships;

(d) document the respective responsibilities of each institution;

(e) with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

Article 18

In respect of transactions or business relationships with foreign politically exposed persons, Member States shall, in addition to the customer due diligence measures set out in Article 11, require obliged entities to:

(a) have appropriate risk-based procedures to determine whether the customer or the beneficial owner of the customer is such a person;

(b) obtain senior management approval for establishing or continuing business relationships with such customers;

(c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;

(d) conduct enhanced ongoing monitoring of the business relationship.

Article 19

In respect of transactions or business relationships with domestic politically exposed persons or a person who is or has been entrusted with a prominent function by an international organisation, Member States shall, in addition to the customer due diligence measures set out in Article 11, require obliged entities:

(a) to have appropriate risk-based procedures to determine whether the customer or the beneficial owner of the customer is such a person;

(b) in cases of higher risk business relationships with such persons, to apply the measures referred to in points (b), (c) and (d) of Article 18.

Article 20

Obliged entities shall take reasonable measures to determine whether the beneficiaries of a life or other investment related insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. Those measures shall be taken at the latest at the time of the payout or at the time of the assignment, in whole or in part, of the policy.

Where there are higher risks identified, in addition to taking normal customer due diligence measures, Member States shall require obliged entities to:

(a) inform senior management before the payout of the policy proceeds;

(b) conduct enhanced scrutiny on the whole business relationship with the policyholder.

Article 21

The measures referred to in Articles 18, 19 and 20 shall also apply to family members or persons known to be close associates of such politically exposed persons.

Article 22

Where a person referred to in Articles 18, 19 and 20 has ceased to be entrusted with a prominent public function by a Member State or a third country or with a prominent function by an international organisation, obliged entities shall be required to consider the continuing risk posed by that person and to apply such appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk. This period of time shall not be less than 18 months.

Article 23

1. Member States shall prohibit credit institutions from entering into or continuing a correspondent banking relationship with a shell bank and shall require that credit institutions take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

2. For the purposes of paragraph 1, "shell bank" shall mean a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

SECTION 4

PERFORMANCE BY THIRD PARTIES

Article 24

Member States may permit the obliged entities to rely on third parties to meet the requirements laid down in Article 11(1)(a), (b) and (c). However, the ultimate responsibility for meeting those requirements shall remain with the obliged entity which relies on the third party.

Article 25

1. For the purposes of this Section, "third parties" shall mean obliged entities who are listed in Article 2, or other institutions and persons situated in Member States or a third country, who apply customer due diligence requirements and record keeping requirements equivalent to those laid down in this Directive and their compliance with the requirements of this Directive is supervised in accordance with Section 2 of Chapter VI.

2. The Member States shall consider information available on the level of geographical risk when deciding if a third country meets the conditions laid down in paragraph 1 and shall inform each other, the Commission and EBA, EIOPA and ESMA to the extent relevant for the purposes of this Directive and in accordance with the relevant provisions of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010, and of Regulation (EU) No 1095/2010, of cases where they consider that a third country meets such conditions.

Article 26

1. Member States shall ensure that obliged entities obtain from the third party being relied upon the necessary information concerning the requirements laid down in Article 11(1)(a), (b) and (c).

2. Member States shall ensure that obliged entities to which the customer is being referred take adequate steps to ensure that relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner are immediately forwarded, on request, by the third party.

Article 27

Member States shall ensure that the home competent authority (for group-wide policies and controls) and the host competent authority (for branches and subsidiaries) may consider that an obliged entity applies the measures contained in Article 25(1) and 26 through its group programme, where the following conditions are fulfilled:

(a) an obliged entity relies on information provided by a third party that is part of the same group;

(b) that group applies customer due diligence measures, rules on record keeping and programmes against money laundering and terrorist financing in accordance with this Directive or equivalent rules;

(c) the effective implementation of requirements referred to in point (b) is supervised at group level by a competent authority.

Article 28

This Section shall not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the obliged entity.

CHAPTER III

BENEFICIAL OWNERSHIP INFORMATION

Article 29

1. Member States shall ensure that corporate or legal entities established within their territory obtain and hold adequate, accurate and current information on their beneficial ownership.

2. Member States shall ensure that the information referred to in paragraph 1 of this Article can be accessed in a timely manner by competent authorities and by obliged entities.

Article 30

1. Member States shall ensure that trustees of any express trust governed under their law obtain and hold adequate, accurate and current information on beneficial ownership regarding the trust. This information shall include the identity of the settlor, of the trustee(s), of the protector (if relevant), of the beneficiaries or class of beneficiaries, and of any other natural person exercising effective control over the trust.

2. Member States shall ensure that trustees disclose their status to obliged entities when, as a trustee, the trustee forms a business relationship or carries out an occasional transaction above the threshold set out in points (b), (c) and (d) of Article 10.

3. Member States shall ensure that the information referred to in paragraph 1 of this Article can be accessed in a timely manner by competent authorities and by obliged entities.

4. Member States shall ensure that measures corresponding to those in paragraphs 1, 2 and 3 apply to other types of legal entity and arrangement with a similar structure and function to trusts.

CHAPTER IV

REPORTING OBLIGATIONS

SECTION 1

GENERAL PROVISIONS

Article 31

1. Each Member State shall establish an FIU in order to prevent, detect and investigate money laundering and terrorist financing.

2. Member States shall notify the Commission in writing of the name and address of the respective FIUs.

3. The FIU shall be established as a central national unit. It shall be responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering or associated predicate offences, potential terrorist financing or are required by national legislation or regulation. The FIU shall be provided with adequate resources in order to fulfil its tasks.

4. Member States shall ensure that the FIU has access, directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks. In addition, FIUs shall respond to requests for information by law enforcement authorities in their Member State unless there are factual reasons to assume that the provision of such information would have a negative impact on ongoing investigations or analyses, or, in exceptional circumstances, where divulgation of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested.

5. Member States shall ensure that the FIU is empowered to take urgent action, either directly or indirectly, when there is a suspicion that a transaction is related to money laundering or terrorist financing, to suspend or withhold consent to a transaction going ahead in order to analyse the transaction and confirm the suspicion.

6. The FIU's analysis function shall consist of an operational analysis which focusses on individual cases and specific targets and a strategic analysis addressing money laundering and terrorist financing trends and patterns.

Article 32

1. Member States shall require obliged entities, and where applicable their directors and employees, to cooperate fully:

(a) by promptly informing the FIU, on their own initiative, where the institution or person covered by this Directive knows, suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing and by promptly responding to requests by the FIU for additional information in such cases;

(b) by promptly furnishing the FIU, at its request, with all necessary information, in accordance with the procedures established by the applicable legislation.

2. The information referred to in paragraph 1 of this Article shall be forwarded to the FIU of the Member State in whose territory the institution or person forwarding the information is situated. The person or persons designated in accordance with the procedures provided for in Article 8(4) shall forward the information.

Article 33

1. By way of derogation from Article 32(1), Member States may, in the case of the persons referred to in Article 2(1)(3)(a), (b), and (d) designate an appropriate self-regulatory body of the profession concerned as the authority to receive the information referred to in Article 32(1).

Without prejudice to paragraph 2, the designated self-regulatory body shall in cases referred to in the first subparagraph forward the information to the FIU promptly and unfiltered.

2. Member States shall not apply the obligations laid down in Article 32(1) to notaries, other independent legal professionals, auditors, external accountants and tax advisors only to the strict extent that such exemption relates to information they receive from or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

Article 34

1. Member States shall require obliged entities to refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have completed the necessary action in accordance with Article 32(1)(a).

In conformity with the legislation of the Member States, instructions may be given not to carry out the transaction.

2. Where such a transaction is suspected of giving rise to money laundering or terrorist financing and where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the obliged entities concerned shall inform the FIU immediately afterwards.

Article 35

1. Member States shall ensure that if, in the course of inspections carried out in the obliged entities by the competent authorities referred to in Article 45, or in any other way, those authorities discover facts that could be related to money laundering or terrorist financing, they shall promptly inform the FIU.

2. Member States shall ensure that supervisory bodies empowered by law or regulation to oversee the stock, foreign exchange and financial derivatives markets inform the FIU if they discover facts that could be related to money laundering or terrorist financing.

Article 36

The disclosure in good faith as foreseen in Articles 32 (1) and 33 by an obliged entity or by an employee or director of such an obliged entity of the information referred to in Articles 32 and 33 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind.

Article 37

Member States shall take all appropriate measures in order to protect employees of the obliged entity who report suspicions of money laundering or terrorist financing either internally or to the FIU from being exposed to threats or hostile action.

SECTION 2

PROHIBITION OF DISCLOSURE

Article 38

1. Obliged entities and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Articles 32 and 33 or that a money laundering or terrorist financing investigation is being or may be carried out.

2. The prohibition laid down in paragraph 1 shall not include disclosure to the competent authorities of Member States, including the self-regulatory bodies, or disclosure for law enforcement purposes.

3. The prohibition laid down in paragraph 1 shall not prevent disclosure between institutions from Member States, or from third countries which impose requirements equivalent to those laid down in this Directive provided that they belong to the same group.

4. The prohibition laid down in paragraph 1 shall not prevent disclosure between persons referred to in Article 2(1)(3)(a) and (b) from Member States, or from third countries which impose requirements equivalent to those laid down in this Directive, who perform their professional activities, whether as employees or not, within the same legal person or a network.

For the purposes of the first subparagraph, a "network" shall mean the larger structure to which the person belongs and which shares common ownership, management or compliance control.

5. For entities or persons referred to in Article 2(1)(1), (2) and (3)(a) and (b) in cases related to the same customer and the same transaction involving two or more institutions or persons, the prohibition laid down in paragraph 1 of this Article shall not prevent disclosure between the relevant institutions or persons provided that they are situated in a Member State, or in a third country which imposes requirements equivalent to those laid down in this Directive, and that they are from the same professional category and are subject to obligations as regards professional secrecy and personal data protection.

6. Where the persons referred to in Article 2(1)(3)(a) and (b) seek to dissuade a client from engaging in illegal activity, this shall not constitute a disclosure within the meaning of paragraph 1.

CHAPTER V

RECORD KEEPING AND STATISTICAL DATA

Article 39

Member States shall require obliged entities to store the following documents and information in accordance with national law for the purpose of the prevention, detection and investigation of possible money laundering or terrorist financing by the FIU or by other competent authorities:

(a) in the case of the customer due diligence, a copy or the references of the evidence required, for a period of five years after the business relationship with their customer has ended. Upon expiration of this period, personal data shall be deleted unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention only if necessary for the prevention, detection or investigation of money laundering and terrorist financing. The maximum retention period after the business relationship has ended shall not exceed ten years;

(b) in the case of business relationships and transactions, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of five years following either the carrying-out of the transactions or the end of the business relationship, whichever period is the shortest. Upon expiration of this period,

personal data shall be deleted, unless otherwise provided for by national law, which shall determine under which circumstances obliged entities may or shall further retain data. Member States may allow or require further retention only if necessary for the prevention, detection or investigation of money laundering and terrorist financing. The maximum retention period following either the carrying-out of the transactions or the end of the business relationship, whichever period ends first, shall not exceed ten years.

Article 40

Member States shall require that their obliged entities have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, or from other authorities, in accordance with their national law, as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship.

Article 41

1. Member States shall, for the purposes of the preparation of national risk assessments pursuant to Article 7, ensure that they are able to review the effectiveness of their systems to combat money laundering or terrorist financing by maintaining comprehensive statistics on matters relevant to the effectiveness of such systems.

2. Statistics referred to in paragraph 1 shall include:

   (a) data measuring the size and importance of the different sectors which fall under the scope of this Directive, including the number of entities and persons and the economic importance of each sector;

   (b) data measuring the reporting, investigation and judicial phases of the national anti-money laundering and terrorist financing regime, including the number of suspicious transaction reports made to the FIU, the follow-up given to these reports and, on an annual basis, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences and the value in euro of property that has been frozen, seized or confiscated.

3. Member States shall ensure that a consolidated review of their statistical reports is published and shall transmit to the Commission the statistics referred to in paragraph 2.

CHAPTER VI

POLICIES, PROCEDURES AND SUPERVISION

SECTION 1

INTERNAL PROCEDURES, TRAINING AND FEEDBACK

Article 42

1. Member States shall require obliged entities that are part of a group to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for anti-money laundering and combating terrorist financing purposes. Those policies and procedures shall be implemented effectively at the level of branches and majority-owned subsidiaries in Member States and third countries.

2. Member States shall ensure that where obliged entities have branches or majority-owned subsidiaries located in third countries where the minimum anti-money laundering and combating terrorist financing requirements are less strict than those of the Member State, their branches and majority-owned subsidiaries located in the third country implement the requirements of the Member State, including data protection, to the extent that the third country's laws and regulations so allow.

3. The Member States, EBA, EIOPA and ESMA shall inform each other of cases where the legislation of the third country does not permit application of the measures required under paragraph 1 and coordinated action could be taken to pursue a solution.

4. Member States shall require that, where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1, obliged entities take additional measures to effectively handle the risk of money laundering or terrorist financing, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country shall consider additional supervisory actions, including, as appropriate, requesting the financial group to close down its operations in the host country.

5. EBA, EIOPA and ESMA shall develop draft regulatory technical standards specifying the type of additional measures referred to in paragraph 4 of this Article and the minimum action to be taken by obliged entities referred to Article 2(1)(1) and (2) where the legislation of the third country does not permit application of the measures required under paragraphs 1 and 2. EBA, EIOPA and ESMA shall submit those draft regulatory technical standards to the Commission within two years of the date of entry into force of this Directive.

6. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 5 in accordance with the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010.

7. Member States shall ensure that sharing of information within the group is allowed provided that it does not prejudice investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities in accordance with national law.

8. Member States may require issuers of electronic money as defined by Directive 2009/110/EC of the European Parliament and of the Council[23] and payment providers as defined by Directive 2007/64/EC of the European Parliament and of the Council[24] established on their territory, and whose head office is situated in another Member State or outside the Union, to appoint a central contact point in their territory to oversee the compliance with anti-money laundering and terrorist financing rules.

9. EBA, EIOPA and ESMA shall develop draft regulatory technical standards on the criteria for determining the circumstances when the appointment of a central contact point pursuant to paragraph 8 above is appropriate, and what the functions of central contact points should be. EBA, ESMA and EIOPA shall submit these draft regulatory technical standards to the Commission within two years of the date of entry into force of this Directive.

10. Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 9 in accordance with the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010.

Article 43

1. Member States shall require that obliged entities take measures proportionate to their risks, nature and size so that their relevant employees are aware of the provisions adopted pursuant to this Directive, including relevant data protection requirements.

   These measures shall include participation of their relevant employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

   Where a natural person falling within any of the categories listed in Article 2(1)(3) performs his professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person.

2. Member States shall ensure that obliged entities have access to up-to-date information on the practices of money launderers and terrorist financers and on indications leading to the recognition of suspicious transactions.

[23] OJ L 267, 10.10.2009, p. 7.
[24] OJ L 319, 5.12.2007, p. 1.

3. Member States shall ensure that, wherever practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided.

SECTION 2

SUPERVISION

Article 44

1. Member States shall provide that currency exchange offices and trust or company service providers shall be licensed or registered and providers of gambling services be authorised.

2. In respect of the entities referred to in paragraph 1, Member States shall require competent authorities to ensure that the persons who effectively direct or will direct the business of such entities or the beneficial owners of such entities are fit and proper persons.

3. In respect of the obliged entities referred to in Article 2(1)(3) (a), (b), (d) and (e), Member States shall ensure that competent authorities take the necessary measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, or holding a management function in those obliged entities.

Article 45

1. Member States shall require the competent authorities to effectively monitor and to take the necessary measures with a view to ensure compliance with the requirements of this Directive.

2. Member States shall ensure that the competent authorities have adequate powers, including the power to compel the production of any information that is relevant to monitoring compliance and perform checks, and have adequate financial, human and technical resources to perform their functions. Member States shall ensure that staff of these authorities maintain high professional standards, including standards of confidentiality and data protection, they shall be of high integrity and be appropriately skilled.

3. In the case of credit and financial institutions and providers of gambling services, competent authorities shall have enhanced supervisory powers, notably the possibility to conduct on-site inspections.

4. Member States shall ensure that obliged entities that operate branches or subsidiaries in other Member States respect the national provisions of that other Member State pertaining to this Directive.

5. Member States shall ensure that the competent authorities of the Member State in which the branch or subsidiary is established shall cooperate with the competent authorities of the Member State in which the obliged entity has its head office, to ensure effective supervision of the requirements of this Directive.

6. Member States shall ensure that competent authorities that apply a risk-sensitive approach to supervision:

   (a) have a clear understanding of the money laundering and terrorist financing risks present in their country;

   (b) have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the obliged entities; and

   (c) base the frequency and intensity of on-site and off-site supervision on the risk profile of the obliged entity, and on the money laundering and terrorist financing risks present in the country.

7. The assessment of the money laundering and terrorist financing risk profile of obliged entities, including the risks of non-compliance, shall be reviewed both periodically and when there are major events or developments in the management and operations of the obliged entity.

8. Member States shall ensure that competent authorities take into account the degree of discretion allowed to the obliged entity, and appropriately review the risk assessments underlying this discretion, and the adequacy and implementation of its policies, internal controls and procedures.

9. In the case of the obliged entities referred to in Article 2(1)(3)(a), (b) and (d) Member States may allow the functions referred to in paragraph 1 to be performed by self-regulatory bodies, provided that they comply with paragraph 2 of this Article.

10. EBA, EIOPA and ESMA shall issue guidelines addressed to competent authorities in accordance with Article 16 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010 on the factors to be applied when conducting supervision on a risk-sensitive basis. Specific account should be taken of the nature and size of the business, and where appropriate and proportionate, specific measures should be foreseen. These guidelines shall be issued within 2 years of the date of entry into force of this Directive.

SECTION 3

CO-OPERATION

SUBSECTION I

NATIONAL CO-OPERATION

Article 46

Member States shall ensure that policy makers, the FIU, law enforcement authorities, supervisors and other competent authorities involved in anti-money laundering and combating terrorist financing have effective mechanisms to enable them to co-operate and co-ordinate domestically concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

SUBSECTION II

CO-OPERATION WITH EBA, EIOPA AND ESMA

Article 47

The competent authorities shall provide EBA, EIOPA and ESMA with all the information necessary to carry out their duties under this Directive.

SUBSECTION III

CO-OPERATION BETWEEN FIUS AND WITH THE EUROPEAN COMMISSION

Article 48

The Commission may lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Union. It may regularly convene meetings with representatives from Member States' FIUs to facilitate co-operation and to exchange views on co-operation related issues.

Article 49

Member States shall ensure that their FIUs co-operate with each other to the greatest extent possible irrespective of whether they are administrative, law enforcement or judicial or hybrid authorities.

Article 50

1. Member States shall ensure that FIUs exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information or investigation by the FIU regarding financial transactions related to money laundering or terrorist financing and the natural or legal person involved. A request shall contain the relevant facts, background information, reasons for the request and how the information sought will be used.

2. Member States shall ensure that the FIU to whom the request is made is required to use the whole range of its powers which it has domestically available for receiving and analysing information when it replies to a request for information referred to in paragraph 1 from another FIU based in the Union. The FIU to whom the request is made shall respond in a timely manner and both the requesting and requested FIU shall use secure digital means to exchange information, wherever possible.

3. An FIU may refuse to divulge information which could lead to impairment of a criminal investigation being conducted in the requested Member State or, in exceptional circumstances, where divulgation of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or the Member State or irrelevant to the purposes for which it has been collected. Any such refusal shall be appropriately justified to the FIU requesting the information.

Article 51

Information and documents received pursuant to Articles 49 and 50 shall be used for the accomplishment of the FIU's tasks as laid down in this Directive. When transmitting information and documents pursuant to Articles 49 and 50, the transmitting FIU may impose restrictions and conditions for the use of that information. The receiving FIU shall comply with those restrictions and conditions. This does not affect the use for criminal investigations and prosecutions linked to the FIU's tasks to prevent, detect and investigate money laundering and terrorist financing.

Article 52

Member States shall ensure that FIUs undertake all necessary measures, including security measures, to ensure that information submitted pursuant to Articles 49 and 50 is not accessible by any other authority, agency or department, unless prior approval is given by the FIU providing the information.

Article 53

1. Member States shall encourage their FIUs to use protected channels of communication between FIUs and to use the decentralised computer network FIU.net.

2. Member States shall ensure that, in order to fulfil their tasks as laid down in this Directive, their FIUs co-operate to apply sophisticated technologies. These technologies shall allow FIUs to match their data with other FIUs in an anonymous

way by ensuring full protection of personal data with the aim to detect subjects of the FIU's interests in other Member States and identify their proceeds and funds.

Article 54

Member States shall ensure that their FIUs cooperate with Europol regarding analyses carried out having a cross-border dimension concerning at least two Member States.

SECTION 4

SANCTIONS

Article 55

1. Member States shall ensure that obliged entities can be held liable for breaches of the national provisions adopted pursuant to this Directive.

2. Without prejudice to the right of Member States to impose criminal penalties, Member States shall ensure that competent authorities may take appropriate administrative measures and impose administrative sanctions where obliged entities breach the national provisions, adopted in the implementation of this Directive, and shall ensure that they are applied. Those measures and sanctions shall be effective, proportionate and dissuasive.

3. Member States shall ensure that where obligations apply to legal persons, sanctions can be applied to the members of the management body or to any other individuals who under national law are responsible for the breach.

4. Member States shall ensure that the competent authorities have all the investigatory powers that are necessary for the exercise of their functions. In the exercise of their sanctioning powers, competent authorities shall cooperate closely to ensure that administrative measures or sanctions produce the desired results and coordinate their action when dealing with cross border cases.

Article 56

1. This Article shall at least apply to situations where obliged entities demonstrate systematic failings in relation to the requirements of the following Articles:

   (a) 9 to 23 (customer due diligence);

   (b) 32, 33 and 34 (suspicious transaction reporting);

   (c) 39 (record keeping); and

   (d) 42 and 43 (internal controls).

2. Member States shall ensure that in the cases referred to in paragraph 1, the administrative measures and sanctions that can be applied include at least the following:

(a) a public statement which indicates the natural or legal person and the nature of the breach;

(b) an order requiring the natural or legal person to cease the conduct and to desist from a repetition of that conduct;

(c) in case of an obliged entity subject to an authorisation, withdrawal of the authorisation;

(d) a temporary ban against any member of the obliged entity's management body, who is held responsible, to exercise functions in institutions;

(e) in case of a legal person, administrative pecuniary sanctions of up to 10% of the total annual turnover of that legal person in the preceding business year;

(f) in case of a natural person, administrative pecuniary sanctions of up to EUR 5 000 000, or in the Member States where the euro is not the official currency, the corresponding value in the national currency on the date of entry into force of this Directive;

(g) administrative pecuniary sanctions of up to twice the amount of the profits gained or losses avoided because of the breach where those can be determined.

For the purpose of point (e), where the legal person is a subsidiary of a parent undertaking, the relevant total annual turnover shall be the total annual turnover resulting from the consolidated account of the ultimate parent undertaking in the preceding business year.

Article 57

1. Member States shall ensure that competent authorities publish any sanction or measure imposed for breach of the national provisions adopted in the implementation of this Directive without undue delay including information on the type and nature of the breach and the identity of persons responsible for it, unless such publication would seriously jeopardise the stability of financial markets. Where publication would cause a disproportionate damage to the parties involved, competent authorities shall publish the sanctions on an anonymous basis.

2. Member States shall ensure that when determining the type of administrative sanctions or measures and the level of administrative pecuniary sanctions, the competent authorities shall take into account all relevant circumstances, including:

(a) the gravity and the duration of the breach;

(b) the degree of responsibility of the responsible natural or legal person;

(c) the financial strength of the responsible natural or legal person, as indicated by the total turnover of that person or the annual income of that person;

(d) the importance of profits gained or losses avoided by the responsible natural or legal person, insofar as they can be determined;

(e) the losses for third parties caused by the breach, insofar as they can be determined;

(f) the level of cooperation of the responsible natural or legal person with the competent authority;

(g) previous breaches by the responsible natural or legal person.

3. EBA, EIOPA, and ESMA shall issue guidelines addressed to competent authorities in accordance with Article 16 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010 on types of administrative measures and sanctions and level of administrative pecuniary sanctions applicable to obliged entities referred to in Article 2(1)(1) and (2). These guidelines shall be issued within 2 years of the date of entry into force of this Directive.

4. In the case of legal persons, Member States shall ensure that they may be held liable for infringements referred to in paragraph 1 of Article 56 which are committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on any of the following:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person; or

(c) an authority to exercise control within the legal person.

5. In addition to the cases referred to in paragraph 4, Member States shall ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 4 has made possible the commission of the infringements referred to in paragraph 1 of Article 56 for the benefit of a legal person by a person under its authority.

Article 58

1. Member States shall ensure that competent authorities establish effective mechanisms to encourage reporting of breaches of the national provisions implementing this Directive to competent authorities.

2. The mechanisms referred to in paragraph 1 shall include at least:

(a) specific procedures for the receipt of reports on breaches and their follow-up;

(b) appropriate protection for employees of institutions who report breaches committed within the institution;

(c) protection of personal data concerning both the person who reports the breaches and the natural person who is allegedly responsible for a breach, in compliance with the principles laid down in Directive 95/46/EC.

3. Member States shall require obliged entities to have in place appropriate procedures for their employees to report breaches internally through a specific, independent and anonymous channel.

CHAPTER VII

FINAL PROVISIONS

Article 59

Within four years after the date of entry into force of this Directive, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and the Council.

Article 60

Directives 2005/60/EC and 2006/70/EC are repealed with effect from [*insert date – day after the date set out in the first subparagraph of Article 61*].

References to the repealed Directives shall be construed as being made to this Directive and should be read in accordance with the correlation table in Annex IV.

Article 61

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by [*two years after adoption*] at the latest. They shall forthwith communicate to the Commission the text of those provisions.

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 62

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union.*

Article 63

This Directive is addressed to the Member States.

Done at Strasbourg,

For the European Parliament	*For the Council*
The President	*The President*

ANNEX I

The following is a non-exhaustive list of risk variables that obliged entities shall consider when determining to what extent to apply customer due diligence measures in accordance with Article 11(3):

(i) The purpose of an account or relationship;

(ii) The level of assets to be deposited by a customer or the size of transactions undertaken;

(iii) The regularity or duration of the business relationship.

ANNEX II

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in Article 14:

(1) Customer risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;

(b) public administrations or enterprises;

(c) customers resident in lower risk geographical areas as set out in paragraph (3).

(2) Product, service, transaction or delivery channel risk factors:

(a) life insurance policies where the premium is low;

(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;

(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;

(e) products where the risk of money laundering/terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money as defined in Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions).

(3) Geographical risk factors:

(a) other EU Member States;

(b) third countries having effective anti-money laundering/combating terrorist financing systems;

(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;

(d) third countries which are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or

monitored in accordance with the Recommendations to ensure compliance with those requirements.

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 16(3):

(1) Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;

(b) customers resident in countries set out in (3);

(c) legal persons or arrangements that are personal asset-holding vehicles;

(d) companies that have nominee shareholders or shares in bearer form;

(e) businesses that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(2) Product, service, transaction or delivery channel risk factors:

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) non-face-to-face business relationships or transactions;

(d) payment received from unknown or un-associated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

(3) Geographical risk factors:

(a) countries identified by credible sources, such FATF public statements, mutual evaluation or detailed assessment reports or published follow-up reports, as not having effective anti-money laundering/combating terrorist financing systems;

(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;

(c) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;

(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

ANNEX IV

Correlation table referred to in Article 60.

Directive 2005/60/EC	This Directive
Article 1	Article 1
Article 2	Article 2
Article 3	Article 3
Article 4	Article 4
Article 5	Article 5
	Articles 6 to 8
Article 6	Article 9
Article 7	Article 10
Article 8	Article 11
Article 9	Article 12
Article 10(1)	Article 10(d)
Article 10(2)	-
Article 11	Articles 13, 14 and 15
Article 12	-
Article 13	Articles 16 to 23
Article 14	Article 24
Article 15	-
Article 16	Article 25
Article 17	-
Article 18	Article 26
	Article 27
Article 19	Article 28
	Article 29
	Article 30

Article 20	-
Article 21	Article 31
Article 22	Article 32
Article 23	Article 33
Article 24	Article 34
Article 25	Article 35
Article 26	Article 36
Article 27	Article 37
Article 28	Article 38
Article 29	-
Article 30	Article 39
Article 31	Article 42
Article 32	Article 40
Article 33	Article 41
Article 34	Article 42
Article 35	Article 43
Article 36	Article 44
Article 37	Article 45
	Article 46
Article 37a	Article 47
Article 38	Article 48
	Articles 49 to 54
Article 39	Articles 55 to 58
Article 40	-
Article 41	-
Article 41a	-
Article 41b	-

Article 42	Article 59
Article 43	-
Article 44	Article 60
Article 45	Article 61
Article 46	Article 62
Article 47	Article 63

Directive 2006/70/EC	**This Directive**
Article 1	-
Article 2(1), (2) and (3)	Article 3(7)(d), (e) and (f)
Article 2(4)	-
Article 3	-
Article 4	Article 2(2) to (8)
Article 5	-
Article 6	-
Article 7	-