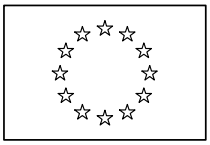


COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 30.6.2009
SEC(2009) 939 final

Commission Staff Working Paper

Compliance with the anti-money laundering directive by cross-border banking groups at group level

Commission Staff Working Paper

Compliance with the anti-money laundering directive by cross-border banking groups at group level

Table of contents

INTRODUCTION

1. Directive 2005/60/EC[1] on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (AML Directive) requires, *inter alia*, EU credit and financial institutions to apply a series of anti-money laundering (AML)[2] measures to prevent the use of the financial system for the purposes of money laundering (see Annex 1 for further detail on the Directive).

2. When complying with these AML measures, credit and financial institutions operating in an EU cross-border context generally develop an AML policy at group level, as part of their global risk management. In late 2008 and early 2009 the Commission services undertook a limited examination on how banks[3] belonging to a group of companies comply, as a group, with their obligations pursuant to the AML Directive[4] and the difficulties they face (see Annex 2 for further detail on the examination and the sources of information). The purpose of the examination was to check whether the fragmentation of national regulation and/or supervision poses a problem for such compliance at group level. In such a case it could undermine the effectiveness of the AML Directive and/or increase the cost of compliance for the institutions acting as a group. It could also result in regulatory arbitrage by criminals.

3. This paper[5] presents the results of that examination. It (1) compares the legislative framework in the AML field with supervisory expectations regarding global AML risk management by banks; (2) presents how banks generally comply with AML measures at group level; (3) describes the costs of compliance; (4) shows the main differences between groups and single institutions, with a particular analysis of the information flows within the group; (5) describes the level of stakeholders' acceptance of the rules; (6) underlines some consistency issues; and (7) finally draws a number of conclusions[6]. This paper is also a preparatory step towards the report on the application of the Directive that the Commission has to submit pursuant to Article 42 of the AML Directive.

---

1 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, OJ L 309 of 25.11.2005, p. 15. This Directive has been incorporated into the EEA-Agreement and is therefore applicable also in Norway, Liechtenstein and Iceland. References in this paper, however, will only be made to the European Union or the European Community.

2 References to money laundering should be understood as, *mutatis mutandis*, also referring to terrorist financing.

3 The survey has focused on banking groups. For the purposes of this paper, banks should be understood as referring to credit institutions as defined in the Article 3(1) of Directive 2005/60/EC.

4 Compliance with other AML legislation will also be considered, where relevant, in this report. This applies for instance to the regulations imposing financial sanctions to terrorists. .

5 This report does not reflect the views of the Commission as such, but rather those of its staff only.

6 The information in this paper is provided to the best of the Commission services' knowledge. References to the national legal framework of the Member States are largely based on information submitted by Member States. They are provided as examples and for illustrative purposes, with no guarantee of being exhaustive or in all cases fully accurate. The Commission services are not responsible for any possible factual inaccuracy.

1. THE ANTI-MONEY LAUNDERING RULES VS. GLOBAL RISK MANAGEMENT: A PROBLEM?

4. **AML preventive policy** generally assumes that: (i) the application by banking institutions of customer due diligence deters criminals from using of the financial system for the purposes of money laundering – thus constituting the main element of the preventive policy; (ii) the identification of suspicious transactions by banks and their subsequent reporting to specialised authorities[7], further to its deterrent effect, assists in the fight against money laundering; (iii) responsible banks able to better identify and monitor risks areas (e.g. applying a risk-based approach) will be able to deliver results regarding the AML preventive efforts; and (iv) risk assessment and management at group level (global risk management) by banks will provide better results than segmented management at local level.

5. The legislation on AML preventive policy is essentially integrated in the AML Directive. This Directive is based on the **territoriality principle** by requiring EU Member States to impose AML preventive obligations on, *inter alia*, the banking institutions established in their territory. These include domestic banks as well as subsidiaries and branches of banks located in other EU Member States (or in third countries), irrespective of whether the parent institution is already subject to the AML requirements of the Member State in which it is located[8]. As a result, a bank, understood as an economic entity, operating in more than one Member State is *de iure* subject to more than one national AML regime within the EU.

6. Although the AML Directive sets a fairly harmonised regime, it only imposes **minimum harmonization requirements** at EU level. This allows for different national AML regimes[9] when implementing the AML Directive[10], including requirements more stringent that those contained in the AML Directive. In this context, **divergent national approaches to regulation**[11] can hinder an effective AML preventive effort by banks acting as a group[12] within the EU. With regard to

---

7 So-called financial intelligence units (FIUs).

8 This contrasts with the so-called "Home Member State principle" which applies in the banking sector. According to this principle, a bank is regulated by the law of its home Member State (normally the one which granted the authorisation) as far as prudential requirements are concerned. Branches of a bank located in other Member States are included in the prudential supervision of the Home Member State of the parent bank. Subsidiaries, on the contrary, are separate legal persons and consequently subject to the home Member State supervision of the State in which they have obtained their authorisation. See Articles 6 to 28 of Directive 2006/48/EC (the banking directive).

9 See for instance, Section 2.2 on the treatment of the client and the transaction, as well as Annex 5.

10 The AML Directive was due to be transposed by Member States by 15 December 2007. Nevertheless, some of them have taken a longer time for adapting their AML national legislation to the novelties of the new AML Directive. For further information o the infringement cases opened by the European Commission for non timely implementation, see the Commission's press releases of 5 June 2008 (IP/08/860), of 16 October 2008 (IP/08/1522) and of 29 January 2009 (IP/09/159).

11 Other important threats to a banking institution effective AML policy would notably be: (i) a sophisticated (from the risk assessment point of view) customer behaviour; and (ii) standard or bureaucratic behaviour of the institutions leading to predictability, in particular resulting from the application (either upon the institution decision or upon regulatory request) of a rule-based approach rather than a risk-based approach.

12 See for instance, the *de Larosière* Group which has recently stated that "*for cross-border groups, regulatory diversity goes against efficiency and the normal group approaches to risk management and capital allocation*". For this Group, such diversity is bound to lead to competitive distortions among financial institutions and encourage regulatory arbitrage. De Larosière Group (2009), p.27.

the scope of the Directive, divergent approaches appear, for instance, on the treatment by Member States of EU banking institutions providing financial services to the residents on their territories, but without a physical establishment in the Member State of the customer. In most Member States[13] the national AML rules do not apply to EU banking institutions[14] providing financial services on their territories in a "free provision of services" basis without physical establishment. On the contrary, in other Member States[15] the national AML law of the State where the customer is located is applicable to EU banks in that situation[16].

7. The territoriality principle of the AML Directive is potentially at odds with the Basel Committee expectation that banks apply a global AML risk management in terms of AML prevention on a groupwide basis, across business lines and geographical locations[17]. This is, in fact, a legislative requirement in at least fifteen EU Member States[18]. In other Member States[19], there is no legal obligation for the parent bank to develop a consolidated groupwide approach to AML risk management but such consolidated approach is *de facto* encouraged by supervisors. This is also in line with the notion of group and the "know-your-structure" principle included in the AML directive[20]. Nevertheless, it must be underlined that, as a result of the territoriality principle of the Directive, these expectations will be supervised locally (i.e. there is no structured approach to EU AML supervision, contrary to the prudential environment), therefore leading to duplications (see Annex 3 for further detail on AML supervision in the EU).

---

13 BE, BG, DE, DL, EL, FI, FR, IE, IT, LT, LU, LV, MT, PL, PT, RO, SE, SK, UK

14 The situation will be different for third country institutions providing cross-border businesses or services in the EU, without physical presence in the EU. For instance, in DE, a Swiss bank in such a situation would need to comply with the German AML law and would be subject to AML supervision by the German supervisor.

15 AT, CY, CZ, EE, ES, HU, LV, NL and SI.

16 In such a situation, the reporting by banks of suspicious transactions to the FIU leads to a paradoxical result: customer due diligence would be conducted according to the rules of the Member State of the customer (and in addition according to the EU Member State of the bank) while filing of reports would be done to the FIU of the Member State where the bank is situated, as mandated by Article 22 of the AML Directive. In this regard, at least two EU Member States (FI, FR) encourage banks in those situations to voluntarily file suspicious transactions reports with the FIU of the Member State of the customer and at least one Member State (CY) requires such filing.

17 See generally Basel Committee (2004).

18 AT, BE, BG, DE, EE, EL, FI, FR, IE, IT, LT, LU, LV, PT and SK

19 CY, CZ, ES, HU, LU (for insurance), NL, MT and UK. In SE there are provisions in the Swedish Financial Supervisory Authority's (FSA) secondary regulation FFFS 2009:1 (which is directly enforceable on all financial institutions and registered companies that it applies to) that one must have a consolidated approach over business lines. The provision in FFS 2009:1 does not apply to subsidiaries and branches in other jurisdictions, but the FSA encourages if the consolidated approach is applied to subsidiaries and branches abroad.

20 See notably Articles 31(1) and 34(2) of the AML Directive. Although the obligations in these articles only concern subsidiaries and branches in third countries, the logic behind both articles is that risk management and AML compliance is conducted at group level irrespective of whether the subsidiaries or branches are located. Indeed, the Directive implicitly integrates the logic of compliance at group level also for subsidiaries and branches located within the EU. While it contains no explicit rules on this, the principle can also be inferred from the rules on the sharing of information regarding money laundering suspicions reported to the financial intelligence units (Cf. Article 28).

8. In this context, any discrepancies between national AML regimes and supervisory practices[21] in a cross-border situation could lead to legal uncertainty and related operational problems (or conversely operational advantages for some). Similar consequences could arise from the application of national bank secrecy (where applicable) and data protection rules.

2. COMPLIANCE BY BANKS AT GROUP LEVEL

9. Banking institutions with branches and subsidiaries outside their Member State of establishment (whether in the EU or outside the EU) are generally organised to manage compliance risk[22] as a group, that is: ensuring that the business complies with existing legislation and regulation, as well as with internal policies and ethical standards. This includes compliance with AML legislation within the EU[23]. This is consistent with the view that global risk management is more efficient[24]: through a centralized system, the flow of information allows the central compliance department to respond faster and more efficiently in case of suspicious of money laundering; the know-how of the parent company can be gradually transmitted to their subsidiaries; and economies of scale can be achieved.

2.1. Internal organisation[25]

10. The central role for AML within banks' organisation is with the anti-money laundering officer[26]. In most countries, the existence of a **MLRO** is compulsory by law[27]. In the case of groups, MLROs will be appointed in each jurisdiction where the group is present, if so required – which is usual – by national legislation[28].

---

21 In its recent report, the *de Larosière* Group stated that "*what seems difficult to contest is that fragmentation in supervision has shown to be the source of major dangers*." De Larosière Group (2009), p.72. Although this comment has been made with regard to prudential supervision in the context of the recent financial crisis, the conclusion could be applied, *mutatis mutandis*, to the AML field.

22 The Basel Committee defines 'compliance risk' as the "*risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities*." See Basel Committee (2005), §3.

23 A recent study conducted for the Commission indicates that trans-national banks (and asset managers) have typically implemented the AML Directive provisions on a group basis. See Europe Economics (2009), §4.62. These findings are consistent with those of a global survey undertaken by a consultancy firm in 2007. In that survey, 94% of the responding internationally active banks from the European region reported that they had a global AML policy in place. 49% of those stated that they had a full global approach (i.e. AML policies and procedures are developed at global level and implemented as consistently as possible worldwide) and 45% reported that they had a hybrid approach (i.e. there is a global AML policy but detailed procedures are set at a regional/local level). Only 6% would have a full AML local approach. According to this survey, "*European banks were significantly more likely than those in other regions to apply a global approach, reflecting the high-level and flexible nature of much European AML legislation*." See KPMG (2007), pp.19 and 52.

24 Implicit in Basel Committee (2004) and Basel Committee (2005) as regards supervisory expectations. Also, information collected by the Commission services from major audit firms supports this opinion.

25 See Annex 4 for further detail.

26 Generally referred to as money laundering reporting officer (MLRO) or money laundering compliance officer (MLCO).

27 For instance, this is the case in at least : AT, BG, DE, EE, EL, FR, LU, MT, PL, SE, SI, SK, UK.

28 Even if not required, in practice banks prefer to have a local MLRO or at least a local "satellite" of the MLRO, who will ac as the key contact for the regulator.

Nevertheless, group compliance officers are typically (but not always) appointed at group level for the internal control and compliance management.

11. The MLRO will normally hold a high position in the firm and be part of the **compliance function**[29] (which normally integrates AML compliance), but the MLRO will not necessarily be the head of compliance. The compliance function is generally seen as playing an important role in the mitigation of reputational risk for the institution[30]. Its importance has grown in recent years[31].

12. For EU banks, the practice is that head office establishes the internal policies and procedures that all the subsidiaries and branches in other EU countries (and in third countries) must implement (without prejudice to the compliance with local rules). This is consistent with the supervisory expectation[32] and with national legislation implementing the AML Directive (as regards third countries)[33]. In doing so, anecdotal evidence suggests that many large banks apply the "higher of home or host" rule to their AML policies and procedures, but recognising that particular local nuances in applicable laws, including data protection legislation, must be considered[34]. Staff of the parent bank periodically revises the implementation of these policies and procedures and test the effectiveness of controls. This may include visits to the countries concerned.

13. Secondly, **vigilant front office and operations staff** are key to banks' AML policy regarding customer acceptance and on-going monitoring for the identification of suspicious activity. Their role is supplemented by sophisticated IT solutions (such as IT monitoring systems) which are increasingly used by banks (in particular large banks) for AML compliance (see below). It is indeed reported that IT solutions are seen as (more or less) necessary to fulfil some compliance activities[35] although human oversight in this area is still significant[36]. In this context, adequate AML training (as well as awareness) of staff is particularly necessary if the bank wants to be able to play an effective role in preventing money laundering. Banks continue to

---

29 The expression 'compliance function' is used to describe staff carrying out compliance responsibilities, without intending to prescribe a particular organisation structure. See Basel Committee (2005), §5.

30 Therefore, one could also assume that some compliance activity is likely to occur in the absence of regulation. See Europe Economics (2009), §3.5.

31 Drivers of this growth include increased regulatory expectations for specific operational compliance activities (notably including AML) and the switching of resources from internal audit to compliance – which in essence, focuses effort towards prevention. See Europe Economics (2009), §3.38. Supervisors are supporting this trend. See generally Basel Committee (2005)

32 See Basel Committee (2004), §8.

33 The Directive requirements concerning the communication of policies and procedures to branches and subsidiaries (cf. Article 34) apply only with regard to third countries, not within the EU. In practice, it is also applied within the EU.

34 Information collected by the Commission services from major audit firms. For global firms, the US or UK requirements are widely used as core standards, but with more detailed policies and procedures at local level reflecting local law. In any event, According to the KPMG 2007 survey, there appears to be a greater willingness in Europe to apply global policies and procedures on a more consistent basis, with less delegation to local operations. This would reflect the high-level principles-based nature of AML requirements in the EU, which makes it easier to design policies and procedures that are flexible enough to be implemented outside the home State. It may also reflect the fact that a common legislative framework applies in Europe and so many of the European respondents find it feasible and economic to implement one set of global policies and procedures. See KPMG (2007, p.20.

35 Europe Economics (2009), §3.49.

36 *Ibid*. §5.40. Also confirmed by KPMG (2007), p.33.

report that properly trained staff is the best AML control and this is reflected in the continued high spending on training programmes in this field[37].

14. The third aspect in the internal organisation is the (internal or external) **audit function**[38] which provides for independent review and test controls after the event. A 2007 survey[39] showed that independent monitoring and testing of AML systems and controls is increasing. It should be noted, in relation to audit, that different national laws foresee a particular role for the external audit on the application of the AML obligations by banks[40] and several countries[41] the law requires banks' external auditors to report on their AML systems and controls on an annual basis. Concerning the audit of a banking group, there do not seem to exist specific rules on the division of duties between the auditor at group level and the auditor(s) at subsidiary level. In practice, the group auditor will often wish to instruct the subsidiary auditor in order to obtain a degree of assurance on the AML provisions at subsidiary level. Particular difficulties have already arisen, as shown by anecdotal evidence, regarding access by the head office auditor to subsidiaries' data on reported suspicious transactions to the FIUs. Auditors are considered to be third parties under Article 28 of the AML Directive and therefore are prevented from accessing to such information. Similar difficulties may arise as a result of bank secrecy rules.

2.2. Treatment of clients and transactions

15. While groupwide internal policies on customer due diligence exist within banking groups[42], the central application of identification/verification measures to clients and/or customer activity monitoring is not common practice – although banking associations tend to consider that such a possibility would be advantageous[43]. The existence of those internal policies does not result either in a uniform application of the internal rules across the group – not least because of the risk-based approach introduced by the Directive: the practical application of the customer due diligence measures will be adapted to local conditions (and regulations) and no box ticking approach followed.

16. Hence, the **client** of one entity within the group is not automatically accepted as client of all entities of the group. If necessary, institutions within a group can cooperate to create an individual customer dossier but the final result will not be automatically shared and is not used to waive the requirements in another

---

37 The importance of training in the banking sector has also been recognised by the 2002 EU Bank Social Partners Joint Declaration on *Lifelong learning in the banking sector*.

38 The Basel Committee recommends that the compliance function and the audit function should be separate, to ensure that the activities of the compliance function are subject to independent review. See Basel Committee (2005), in particular principle 8 (relationship with internal audit).

39 KPMG (2007), p.21 and seq.

40 It should not be forgotten that auditors are themselves subject to the AML obligations of the Directive.

41 At least in BE, DE, ES, LU, PT, SK.

42 Indeed, the AML Directive requires banks to communicate relevant policies and procedures of customer due diligence to branches and (majority owned) subsidiaries. This is explicitly requested with regard to branches and subsidiaries in third countries (cf. Article 34) and implicitly with regard to branches and subsidiaries within the EU. This is also a supervisory expectation, see Basel (2004), §10 and seq.

43 Interestingly, the Basel Committee also advanced in 2004 that complementing monitoring of accounts and transactions at local level with aggregated monitoring at the centralised site would provide banks with the opportunity to monitor for patterns of suspicious activity that cannot be observed from the local side. See Basel (2004), §16.

jurisdiction. Indeed, national requirements may differ as to the level or detail of customer due diligence measures to be conducted or as to the approaches to information data collection and retention (see Annex 5 for further detail and Section 4 on the flows of information within the group).

17. If a customer is transferred within the group, different situations apply to branches and subsidiaries located in the EU. In the case of a branch's customer, a bank may in principle rely on already existing identification data held by the branch provided it is up-to-date and fulfils the requirements set out in the destination State legislation. This is so because the branch is the same legal person as the parent institution, therefore rights and obligations are generated by the bank itself. In the case of subsidiaries in the EU, normal rules on relations with third parties will apply[44]. No specific provisions foreseeing a special treatment for customers introduced by/to subsidiaries have been enacted by national legislation – though the application of the risk based approach and the intra-group information flows could facilitate the customer acceptance process in such a situation.

18. Politically exposed persons (PEPs) and sanctions lists are two areas where banks are making an effort to apply a group policy, though local requirements must also be followed. Banks increasingly establish specific procedures to identify (essentially relying on commercial lists of PEPs) and monitor PEPs on an on-going basis, with a view to apply enhanced customer due diligence measures, as mandated by the Directive. Concerning sanctions lists, it appears that, although they can be provided by the parent bank, they are as a general rule applied by each bank according to local rules. However, many banks would voluntarily apply, to the extent permitted by personal data protection legislation, the sanction lists of the countries where they operate in order to mitigate risks (see Annex 5 for further detail).

19. In cross-border situations, the **monitoring of customer activity** is conducted directly by the institutions at local level, even if policies and procedures are normally validated by the parent bank. Banking associations refer to local regulatory requirements as a barrier for a further integrated approach (see also section 4 on flows of information). Thus, monitoring at group level is only used for subsidiaries and branches within the same jurisdiction. Different methods are used by banks for customer monitoring. In addition to vigilant staff, there is, despite of the cost, an increased use of sophisticated IT monitoring systems allowing for the screening of high volumes of transactions (see section 3 on cost of compliance). The human resources implications of these systems must not be underestimated (for instance the analysis of potentially suspicious transactions, the need to review false positives, etc). The challenge for banks is to adapt these systems to the right money laundering trends and typologies[45], for which intelligence sharing with the public sector is key (see section 5 on acceptability).

20. Concerning the **analysis of detected transactions**, national legislation does not contain, in general, provisions requiring that such analysis is conducted at group

---

44 See Annex 5 for further detail.

45 Customer monitoring with a view to identify terrorist financing patterns is particularly difficult, notably because of the small value of the associated transactions. In this case, it is reported that enhanced transaction monitoring alone is unlikely to prove a solution to these difficulties, which triggers the need for increased intelligence sharing between the public and the private sector

level and it appears to be largely dealt with at local level. The possibility of undertaking such analysis at group level would depend of the possibility to exchange information between parent and subsidiaries/branches on suspicions (see section 4). The filing of "suspicious transaction reports/suspicious activity reports" with the FIUs, follows local laws and procedures. National legislation in EU countries does not require the parent bank to report to the FIU (or to the supervisor) of its own Member State about reports filed by their branches or subsidiaries in other Member States[46]. This is normally not done on a voluntary basis either, unless in exceptional cases when there is a serious reputational risk for the group (see also Annex 5).

3. THE COST OF COMPLIANCE

21. The cost of compliance with AML requirements is not insignificant and has increased in recent years following the regulatory changes introduced in the EU, notably the AML Directive[47]. A recent external study has examined for the Commission the cost of compliance for certain types of firms within the financial industry (notably including banks[48]) with six key EU directives in the financial services area, including the AML Directive[49]. The study focuses on the so-called 'incremental compliance costs' caused by these directives, not on the total costs of activities that happens to contribute to regulatory compliance.

22. The study identifies separately cost impacts that are of one-off nature (i.e. those costs that only have to be incurred once in making the transition, such as IT investment and the re-shaping of business processes) from those that are recurring in nature (on-going costs as a result of regulation). The one-off costs of compliance with the AML Directive for banks, financial conglomerates and investment banks roughly account for 10% of all their financial services regulatory costs; while in the case of on-going costs of compliance, the percentage increases to around 13%.

23. The main source of AML related compliance spending is on IT. Concerning the one-off costs, this included projects designed to: (i) meet the "Know-Your-Customer" requirements; (ii) facilitate increased monitoring of suspicious transactions through increased automation of processes; (iii) facilitate PEPs screening; and (iv) assist in risk assessment. Regarding the on-going costs, most of the IT expenditure is linked to access costs to various databases dedicated to the tracking and screening of relevant parties such as PEPs, watch lists etc. Whilst some firms (generally larger banks) see automation as the only way to provide the necessary evidence of an audit

---

46 A paradoxical case may arise when the bank has no branch or subsidiary in a State where it provides financial services. In such a situation, it would report to the FIU of its own Member State about suspicious transactions. See section 1 on this point.

47 See Annex 6 for further detail. However, one would also need to consider that the cost of complying with AML measures in a non-harmonised environment would be higher.

48 The study makes no distinction between banks with cross-border activities or local banks, but most of the banks surveyed have cross-border activities and would typically have a group compliance policy regarding AML requirements.

49 Europe Economics (2009). The survey concentrated on firms from four sectors within the financial services industry in the EU: banks and financial conglomerates, asset managers, investment banks and financial markets. The six directives concerned are the so-called Prospectus Directive, the Financial Conglomerates Directive, the Capital Requirements Directive, the Transparency Directive, the Markets in Financial Instruments Directive – MiFID and the AML Directive.

trail to the regulatory authorities in the event of problems arising (as well as being cost effective by comparison to manual effort), a number of firms have retained significant (or total) human oversight in this area.

Training and (for larger banks) external consultants are also important sources of costs.

4. THE QUESTION OF THE CROSS-BORDER INTRA-GROUP FLOW OF INFORMATION

24. When compared to individual banks, banking groups complying with the AML Directive at group level do not seem to enjoy particular advantages as regards the treatment of the client (see section 2)[50]. The main difference for groups, compared to individual banks, is the question of the **cross-border intra-group flow of data**, both on the clients and on suspicions.

25. Indeed, supervisors attach particular importance to the question of cross-border intra-group sharing of information, in particular on higher risk customers and activities relevant to the global management of reputational and legal risks[51]. This question is possibly the most difficult one for banks when implementing an AML compliance policy at group level. The main reason for this is the balance between the AML requirements, on the one hand, and the personal data protection legislation and/or banking secrecy regulations, on the other hand (see section 6 on consistency issues).

26. The main difficulty applies to the intra-group sharing of information on the customer and on the detected suspicious transactions[52], prior to the formalisation of a report to the FIU (or the decision not to make one). In principle, national AML legislation does not explicitly restrict the intra-group flows of **information regarding customers** for the purposes of applying customer due diligence measures. In practice, however, the perception of the banking associations is that, in the majority of cases, flows of information within the group with regard to customers would not take place due to the requirements resulting from national legislation on data protection[53] (or its application) and on banking secrecy (where they exist). Anecdotal evidence suggests that banking groups tend to overcome these difficulties through on-site visits by head office/parent bank staff, who then are able to report back to headquarters[54].

---

50 Concerning the impact on employees, anecdotal evidence provided to the Commission services suggests that being part of a group may result in better protection for employees in case of external harassment or threat, as employees may be easily moved within the group to another geographical location, if need be.

51 See Basel Committee (2004), §§17-19. In particular the Basel Committee recommends that the "*bank's centralised KYC function should evaluate the potential risk posed by activity reported by its branches and subsidiaries and where appropriate assess its world-wide exposure to a given customer*." *Ibid*. §18.

52 See Annex 5 for further detail on this issue.

53 The protection of personal data is a fundamental right of the person which is expressly laid down in Article 8 of the Charter of Fundamental Rights of the European Union and in the European Convention of Human Rights (Art. 8). Legislation adopted by the European Union in the field of data protection lays down the principles that the processing of personal data shall comply with in order to respect this fundamental right.

54 This situation does not seem to match the Basel Committee expectations on the removal of "legal impediments" to intra-group sharing of information (see Basel Committee (2004), §§24-27, in particular

27. An adequate **treatment of suspicious cases** within a banking group, aiming at determining whether the filing of a suspicious transaction report is necessary, would require an information exchange with other entities within the group on the suspicious case (as well as on previous suspicious transaction reports established on the same customer within the group). Nevertheless, in some Member States[55] this is not possible unless a report to the FIU has been previously formalised. In practice, according to the banking associations, information on suspicious cases is rarely shared within the group: only in exceptional cases, covered by agreements/protocols under the control of the parent bank that guarantee confidentiality and secure transmission of data. The perception of banking associations in this regard is that national data protection and bank secrecy rules would generally prevent the circulation of such data between institutions of the same group.

28. The possibility of circulating within the banking group information on **reports filed with the FIUs** is provided for in Article 28(3) of the AML Directive[56]. However, EU FIUs are not enthusiastic about such possibility[57].

29. In principle, no restrictions exist for the circulation of information within the banking group about **trends, typologies or general feedback** received from FIUs or other public authorities, provided it does not include precise information on clients or their transactions related to on-going procedures. The situation concerning feedback on on-going particular cases including data on clients and transactions – when provided[58]– is less clear. Nevertheless, national AML legislation is in most cases silent and thus open to interpretation[59]. In some cases, circulation of information would only be possible with the express authorisation of the FIU[60] – otherwise, the information should remain with the AML compliance department of the reporting entity[61]. In any event, general rules on data protection and bank secrecy would apply.

---

§27). At the same time, it is unclear whether the Basel Committee took into account in that paper the fundamental right dimension of the legislation on the protection of personal data.

55 FI, PL, SK. In NL, the law requires that the report with the FIU is done immediately. Therefore, de facto it is not possible to share information within the group before formalising the report.

56 Almost all Member States have integrated this provision in national law. One Member State (SI), however, decided not to allow for the intra-group disclosures relating to reports filed with the FIU (with regard to disclosures between parent bank and subsidiary. However, information flows between branch and head office are possible)

57 See EU FIU Platform (2008a), p.14-16. FIUs also underline that there is a risk of abusing the permission for this kind of intra-group exchanges of information and of circumventing other prohibitions of disclosure: e.g. in order to circumvent the prohibition to provide information following a request by the judicial authorities, banks could disclose the same information to the FIU and then pretend to be entitled to circulate the information within the group. *Ibid*., p.16. See also Annex 5, section D iii).

58 This type of specific feedback is not always provided by FIUs. In some cases, feedback is limited to either general feedback or to publicly available information (e.g. outcome of the judicial procedures).

59 Only in a few countries (DK, HU, LU, LV, SK) national legislation would explicitly allow for the intra-group circulation of such feedback. On the contrary, in one Member State (NL), legislation explicitly foresees that FIU feedback with regard to specific reports cannot be disclosed within the institutions belonging to the same group, only the report itself can be.

60 FIUs are, in general, not too favourable to the disclosure of feedback within the banking group. See EU FIU Platform (2008), p.13-14.

61 BG, CY, FI, RO, UK

30. Concerning **record keeping**, banking associations report that, due to regulatory requirements[62], information is archived in each local jurisdiction, without connection between databases. As a result, centralised archiving at group level of the information collected by different Member States is not really possible, although it could be an efficient way of ensuring that records are easily retrievable and logged[63].

5. ACCEPTABILITY OF AML OBLIGATIONS

31. There appears to be a **broad support** from EU banks (whether acting cross-border or not) concerning the EU AML regulatory framework. A recent study conducted for the Commission[64] reports that the majority of interviewees viewed the AML Directive as useful and effective in deterring money laundering as well as maintaining market confidence. This is consistent with the opinions expressed in an independent survey conducted in 2007[65]. According to this survey, the majority of banks in Europe believe that their current legislative and regulatory burden is acceptable (although they also state that the content of existing legislation requires improvement if money laundering is to be effectively tackled in the region)[66].

From the **cost perspective**[67], another study conducted for the Commission[68] shows that banks seemed to have successfully integrated the rules into their daily business. The majority of the surveyed participants viewed the AML regime as an inevitable part of "business as usual"[69]. A few believe there would be benefits in being "ahead of the game" in this regard (for instance, from the perspective of better managing reputational risk). It is noteworthy, however, that a small number of surveyed

---

62 For instance, in two Member States (ES and SI) the data retention period is longer (6 years) than the one foreseen in the Directive (5 years).

63 This also implies that it is not possible for an institution to organise a centralised system covering operations in different Member States in order to comply with the requirements of Article 32 of the Directive. There are efficiency arguments in favour of such a centralised system: for instance, a centralised system would ensure a consistent approach and the smooth the transfer of knowledge around requests for information from local FIUs. At the same time, the key factor is that the information can be retrieved quickly, rather than the actual location of the records.

64 CRA International (2009), p.13 and section 3.7.3. The CRA International study focuses on the Financial Services Action Plan of 1999, so that in principle the AML Directive concerned was the one of 2001 (so-called second AML Directive). However, to the extent that the second AML Directive has been repealed in the meantime by Directive 2005/60/EC (so-called third AML Directive), it is difficult to disentangle the impacts of the second and the third Directives (see section 3.7)

65 KPMG (2007), p. 54.

66 A different survey conducted on UK financial services businesses (not limited to banks), also showed that an overwhelming majority of respondents were satisfied or very satisfied their organisation had successfully implemented the risk based approach to anti-money laundering requirements. The industry perception was also that any organisation that is non-compliant in the AML area is an industry outlier and vulnerable to severe regulatory sanction, such as public censure and financial penalties. See PWC (2007b), pp.3 and 6.

67 A previous independent survey conducted in 2007 on UK financial services businesses (not limited to banks) showed a negative perception of the cost-benefits derived from the new AML rules to the date of the survey. The audit firm which undertook the survey concluded that demonstrating the efficiencies that the regime is intended to deliver to businesses would become increasingly challenging. PWC (2007b), pp.3-4.

68 Europe Economics (2009), §5.35.

69 A not uncommon view would be that its ongoing incremental impact of the Directive would have been slight (or even negative) were it not for the broadened scope (to include, for instance, Politically Exposed Persons). *Ibid.*

institutions regard the anti-money laundering regime in general as involving costs disproportionate to any plausible beneficial effect.

32. The flexibility provided by the **risk-based approach** introduced by the Directive seems to be one, if not the main, of the drivers for this level of acceptability, as confirmed by the study on cost of compliance[70] and an independent survey[71]. It has been anticipated[72] that the application of the risk-based approach will lead to even greater involvement and responsibility of senior management in AML issues, which possibly plays a role in this level of acceptability. At the same time, the application of the risk-based approach increases the firm's responsibility and the consequent need for being able to provide to the regulatory authorities the necessary evidence of the choices made. This has led some firms (generally large banks) to see automation as the only way to demonstrate to the authorities – should a problem arise – that the firm had done all that it reasonably could[73].

33. Concerning specifically the EU **cross-border dimension**, this level of acceptability is confirmed by the absence of formal or informal complaints with national authorities on specific difficulties to apply the AML rules at group level within the EU[74].

34. Rather than at the AML rules themselves, stakeholders point at their interaction with other legislation, such as data protection and bank secrecy rules (see section 6) or at the practical application of some of their aspects. Industry points at the need to ensure **cooperation and intelligence sharing between the private and the public sector** – which could also be shared at group level. In a recent study conducted for the Commission[75], as much as 93% of the interviewees considered feedback to their institutions as an essential part of a good AML policy and estimated that more substantial feedback is required from FIUs and law enforcement authorities. Such feedback should in particular help them in having a clearer understanding of the typologies used or the main threats. While providing feedback to banks is an obligation contained in the Directive, its practical implementation could be improved[76]. Indeed, that study concludes that more and better feedback should be provided to credit and financial institutions, which should receive a priority treatment from FIUs and law enforcement authorities compared to the other entities and persons reporting to them.

---

70 *Ibid*.

71 According to the KMPG survey, the broad support for the regulatory framework in Europe is likely to be attributable to the flexible, risk-based approach that has been incorporated into the EU AML Directive, as well as the degree of consultation that has taken place between the Commission, regulators and banks in writing the Directive. See KPMG (2007), p.54.

72 KPMG (2007), p. 12.-13. According to KPMG, this also raises questions about the level of engagement that regulators expect senior management to have in each of the processes underlying the risk-based approach, from risk management through to design, implementation and oversight of controls.

73 Europe economics (2009), §§4.59 and 5.40.

74 Some Member States (PT,FR) have reported about difficulties met by banking institutions regarding the flow of information with their branches and subsidiaries in third countries

75 See generally B & S Europe (2009). The survey in this study also encompasses non-financial entities or persons. See also KPMG (2007), p.36.

76 The EU FIUs have also underlined the importance of feedback in a recent report. This report provides a brief overview of the existing regulatory framework and analyses different types of feedback from the FIU perspective. See generally EU FIU Platform (2008b).

6. CONSISTENCY ISSUES

6.1. AML supervision

35. As explained in §8, there is a risk that decentralised competing supervision of AML compliance by banking groups could lead to conflicting supervisory views, although in practice, there is no evidence of this happening. Financial services supervisors, in particular banking supervisors, are enhancing their cooperation on AML issues, e.g. within the AML task force created by CEBS, CEIOPS and CESR. At the same time, not all banking supervisors have the power to cooperate and exchange AML related information on supervised institutions with foreign authorities tasked with AML supervision[77]. CEBS has recently recognised that there is a case for initiating further work regarding the effectiveness of supervision in the implementation of the AML Directive and proposed that the AML task force of CEBS, CEIOPS and CESR takes this work forward[78].

6.2. AML and data protection

36. The link between the AML rules (and supervision) and the data protection rules (and supervision) also give rise to problems of consistency. Stakeholders underline the need to clarify the interpretation of some data protection rules in the specific framework of the prevention of money laundering and to provide the necessary guidance. This is also due to the fact that the wording of some provisions of the AML Directive, for instance CDD requirements, is not sufficiently precise and leaves room for discretion, which may give rise to different interpretations with regard to the extent of these obligations and may create uncertainty about the amount and the degree of personal information they have to collect to comply with AML requirements.

37. Different issues have arisen in connection to the intra-group exchange of information within the EU[79] (see Annex 7 for further detail). The main difficulties relate to the exchange of information on the customer either for the purposes of customer acceptance policy or for the customer and transaction monitoring. Stakeholders would welcome clarification as to whether a systematic sharing of customer information within the group is compatible with data protection legislation, in particular with the principles of purpose limitation, necessity, proportionality and appropriate legal basis for the processing, or whether a case-by-case justification would be needed. In the latter case, stakeholders tend to consider that the customer and transaction monitoring at group level would not be practical. This question has particular importance given the application of the risk-based approach. In the same manner as banks need to demonstrate to the banking supervisors that the extent of the customer due diligence measures is appropriate in view of the risk of money laundering, banks would also need to justify to the data protection authorities that the processing in question, involving intra-group and cross-border transfer of information, complies with the data protection principles of necessity,

---

77 CEBS (2009), p.48.

78 *Ibid*., p.49.

79 The transfer of personal data to an entity of the group in a third country poses particular challenges for the intra-group sharing of information, such as the question of the adequate level of protection in that third country etc. However, this question is beyond the scope of this paper.

proportionality, purpose limitation and appropriate legal basis for the processing. Also, the legal coverage of the consolidated sanctions lists (e.g. aggregating national lists applicable in the countries where the banking group is present) is unclear for stakeholders.

Concerning the intra-group transfer of information on suspicious transactions and on reports thereof, a question arises as to whether the absence of prohibition in the national legislation transposing the AML Directive is a sufficient legal basis for the transfer of data within the banking group from the point of view of data protection rules. An additional issue raised in connection to the processing of suspicious transactions is that the intra-group circulation of information or the record keeping at group level should not amount to blacklisting of a customer.

38. Clarifying the interpretation of these issues would also increase the predictability of the positions of the data protection authorities in this area. The overall goal should be to increase the legal certainty for institutions subject to the AML requirements, so that these institutions can effectively exchange information within the group, when needed for the prevention of money laundering, whilst complying with data protection legislation.

39. Nevertheless, it appears that at present, national data protection authorities and financial services supervisors do not liaise enough in the AML field. Only in one Member State[80] is there a specific code of conduct for the banking sector which makes clear how the sector should ensure compliance with data protection rules. It has been suggested in this context that there would be an EU added value if clarification or guidance is addressed at EU level. Indeed, some preliminary work to that end has been undertaken by the Commission services in 2008 within the framework of the Article 29 Working Party. Work is still on-going[81].

6.3. Bank secrecy rules

40. The question of national bank secrecy rules has also been raised. While in principle Member States have committed to make sure that bank secrecy rules do not inhibit implementation of AML rules[82], in practice some difficulties remain. Difficulties relate, for instance, to the sharing of information on the customer and the suspicion before making a report to the FIU[83]. In some Member States[84] banks may not disclose information covered by the bank/professional secrecy rules (e.g. obtained in the course of a business relationship) to its parent company/subsidiary[85] if the

---

80 NL.

81 A consultation paper prepared by the Commission services on Processing of personal data and the EU anti-money laundering rules was submitted to the Article 29 Data Protection Working Party. This Working Party, created by Article 29 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

82 See Recommendation 4 of the FATF, endorsed by EU Member States: "*Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF recommendations*".

83 Article 28(3) of the AML Directive waives any bank secrecy rule opposing to the sharing of data once the report made.

84 AT, BG, FR, MT, PT, SI

85 National rules generally prohibit disclosure to “third parties”. In this regard, it is difficult to consider that a branch is a third party to the head office of the same institution. As a result, the bank secrecy rules

information is on a customer who is not under suspicion, unless the customer consents to this[86]. In other Member States, disclosure is possible only if justified by the "need-to-know" principle[87] or if equivalent rules on bank secrecy are in force in the destination State[88].

41. Nevertheless, the bank secrecy rules in some Member States explicitly provide for intra-group flows of information for the purposes of money laundering prevention[89] or do not constitute an obstacle to them[90]. In other Member States[91] there are no bank secrecy rules in national legislation, but a confidentiality duty arises from the contractual obligation between customer and bank. Still, it might be possible that in some jurisdictions[92] disclosure of information within a group, where this involves disclosure to a separate company, may constitute a breach of secrecy.

CONCLUSIONS

42. This paper shows that, despite the minimum harmonisation nature of the AML Directive, the degree of convergence across Member States AML rules applying to banks is relatively high[93]. Nevertheless, national regulatory differences remain in certain areas. This is the case, for instance, regarding: (i) the scope of national legislation which applies to banks established in other EU Member States and providing financial services cross-border in a "free provision of services" basis without establishment (see §6); (ii) the level or detail of customer due diligence measures to be conducted, such as the formalities and requirements on customer identification or the requirements for simplified/enhanced customer due diligence (see §16 and Annex 5); or (iii) differences regarding the extent of data that can circulated within the banking group (see section 4 and Annex 5). Nevertheless, the main AML-related barriers to banks' undertaking cross-border business and applying an AML policy at group level will often be of practical rather than of legal nature.

43. Some uncertainties remain, in particular, regarding the interaction of AML rules with national data protection rules and with bank secrecy rules (see sections 6.2, 6.3, and Annex 7) and their impact on banks' AML policies at group level, especially regarding the information flows within the group. In this context, the Commission services have launched exploratory work with the EU data protection authorities within the so-called Article 29 Working Party with a view to achieve more clarity, at

---

would not apply to intra-institution flows of information, even if cross-border. They would, on the contrary apply to the relation parent bank-subsidiary.

86 PT, SI.

87 DK.

88 FI.

89 CY, HU (if written consent of the customer), LU, RO, SE.

90 CZ, EE, ES, IE (based on common law, not statutory rules), PL, SK

91 BE, DE. IT, NL, UK

92 NL, UK.

93 See also KMPG (2007), p.20: "*In Europe, there appears to be a greater willingness to apply global policies and procedures on a more consistent basis, with less delegation to local operations. This is likely to reflect the high-level principles-based nature of AML requirements in this region, which makes it easier to design policies and procedures that are flexible enough to be implemented outside the home country. It may also reflect the fact that a common legislative framework applies in Europe and so many of the European respondents find it feasible and economic to implement one set of global policies and procedures*".

EU level, on the interrelations between AML rules and data protection rules. Work is still on-going.

44. This paper also shows that promoting further convergence between EU supervisors on supervisions of banks' compliance with the AML rules is desirable (see section 6.1). Indeed, CEBS recently concluded that there is a case for further work within the AML task force of CEBS, CESR and CEIOPS on the effectiveness of supervision in the implementation of the AML Directive[94]. The importance of supervision to promote, *inter alia*, integrity in the financial system was recently recalled by the Group of Twenty (G-20)[95].

[94] CEBS(2009), p.49

[95] Group of Twenty (2009a), §13 and seq.

ANNEX 1 – THE AML DIRECTIVE

Directive 2005/60/EC[96] on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (the "AML Directive") requires, *inter alia*, credit and financial institutions to apply a series of preventive measures with a view to prevent money laundering and terrorist financing.

The main obligations resulting from the AML Directive are the following:

(1) Customer due diligence (CDD). Credit and financial institutions should apply CDD measures when establishing a business relation with a client (and also in other circumstances, see Article 7). Customer due diligence measures – also referred to as "know your customer" (KYC) – imply (Article 8): (i) the identification of the customer and verification his/her identity; (ii) the identification of beneficial owner (where applicable); (iii) obtaining information on the purpose and intended nature of the business relationship; and (iv) conducting on going monitoring of the business relationship. CDD measures may be adapted depending on the risk perceived (risk-based approach). The Directive mandates or allows for simplified CDD (Article 11): mandated when the client is a credit or financial institution and allowed in cases decided nationally in accordance with the cases or conditions set out in the Directive or its implementing legislation[97]. The Directive also requires the application of enhanced CDD in certain cases (Article 13), namely regarding: non-face to face situations; relationships with politically exposed persons (PEPs), and correspondent banking relationships with banks in third countries). In some cases the Directive allows for the performance of CDD measures by third parties under certain conditions (Articles 14 to 19). Failure to satisfy the CDD requirements should imply that no business relationship is entered into (Article 9). The Directive is worded in relatively broad terms which may give rise to different interpretation and application of the requirements of this obligation.

(2) Reporting obligations. Credit and financial institutions are required to inform the national financial intelligence units (FIUs) of transactions/situations where there is a suspicion that money laundering is being or has been committed or attempted (Article 22). Concerned transactions should, as a matter of principle, not be carried out before filing the report (Article 24). Credit and financial institutions should not disclose to the customer (so-called prohibition of tipping off) that a report has been filed with the relevant FIU. They should not disclose this fact to third parties either, except when authorised by the directive (Article 28). FIUs may request the credit and financial

---

96 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, OJ L 309 of 25.11.2005, p. 15.
See: http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm
See also the summary of this Directive in Scadplus: http://europa.eu/scadplus/leg/en/lvb/l24016a.htm

97 Directive 2006/70/EC of the European Commission 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, OJ L 214, 4.8.2006, p.29.
See: http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm

institutions to provide additional information (Article 22). Disclosure in good faith should not constitute a breach of any legislative obligation and should not imply liability of any kind (cf. Article 26). Credit and financial institutions' employees making suspicious reports should be protected from threat and hostile action (cf. Article 27).

(3) Record keeping. Credit and financial institutions should keep documents and information relating to the above for at least 5 years (Article 30). Additionally, credit and financial institutions should have systems in place that enable them to reply fully and rapidly to enquiries from FIUs or other authorities as to whether they maintain or have maintained during the previous 5 years a business relationship with specified legal or natural persons and on the nature of the relationship (Article 32).

(4) Internal policies and procedures. Credit and financial institutions should establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication (Article 34).

(5) Awareness and training. Credit and financial institutions should take appropriate measures so that their relevant employees are aware of the provisions in force on the basis of this directive, including participation in training programs (Article 35).

(6) Supervision. Credit and financial institutions should be supervised on their compliance with the directive rules (Article 37). There are penalties for lack of compliance (Article 39).

ANNEX 2 – THE EXAMINATION

The Commission services undertook in late 2008 and early 2009 a limited examination on compliance at group level with the AML Directive by banking institutions.

This survey included an information-gathering exercise involving selected stakeholders:

- Member States AML authorities were consulted through the Committee for the Prevention of Money Laundering and Terrorist Financing referred to in Article 41 of the AML Directive. All Member States replied to the questionnaire.

- National financial services supervisory authorities were also contacted through the Anti-Money Laundering Task Force (AMLTF) created by the 3 Committees regrouping the national supervisors: CEBS[98], CESR[99] and CEIOPS[100]. 11 national supervisors from the following countries provided replies to the questionnaire on supervisory issues: Austria, Belgium, Cyprus, Greece, Finland, Italy, Latvia, Lithuania, Malta, Netherlands and Slovenia. Results of own research undertaken by the AMLTF has also been used, where appropriate.

- The following associations representing credit institutions have also provided replies to a questionnaire or expressed their opinion on the survey[101]: EBIC (European Banking Industry Committee), EBF (European Banking Federation) EAPB (European Association of Public Banks), ESBG (European Savings Banks Group), EACB (European Association of Cooperative Banks), and BBA (British Bankers Associations). Some individual banks also provided comments to the Commission services.

- The European Contact Group representing large audit firms active in auditing credit and financial institutions. Members of two large networks of auditing firms replied to the specific questionnaire, covering in aggregate, a large number of Member States: Austria, Belgium, the Czech Republic, Denmark, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Poland, Portugal, Slovakia, Spain, Sweden and the United Kingdom.

---

98 The Committee of European Banking Supervisors (CEBS) was created by Commission Decision 2004/5/EC of 5 November 2003 *establishing the Committee of European Banking Supervisors*, OJ L 3, 7.1.2004, p. 28. In the meantime, Decision 2004/5/EC has been repealed by Commission Decision 2009/78/EC of 23 January 2009 *establishing the Committee of European Banking Supervisors*, OJ L 25, 29.1.2009, p. 23. See www.c-ebs.org

99 The Committee of European Securities Regulators (CESR) was created by Commission Decision 2001/527/EC of 6 June 2001 *establishing the Committee of European Securities Regulators*, OJ L 191, 13.7.2001, p.43. In the meantime, Decision 2001/527/EC has been repealed by Commission Decision 2009/77/EC of 23 January 2009 *establishing the Committee of European Securities Regulators*, OJ L 25, 29.1.2009, p. 18. See: www.cesr.eu

100 The Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS) was created by Commission Decision 2004/6/EC of 5 November 2003 *establishing the Committee of European Insurance and Occupational Pensions Supervisors*, OJ L 3, 7.1.2004, p. 30. In the meantime, Decision 2001/527/EC has been repealed by Commission Decision 2009/79/EC of 23 January 2009 establishing the Committee of European Insurance and Occupational Pensions Supervisors, OJ L 25, 29.1.2009, p. 28. See www.ceiops.eu

101 This survey also builds on previous exchanges during 2007 and 2008 between the Commission services and the associations representing credit institutions.

- Member States data protection authorities were contacted through the so-called Article 29 Working Party[102]. The work of the Article 29 Working Party is still on-going.

The Commission services also used the results of two studies recently commissioned by the Commission (DG Internal Market and Services) regarding the application of financial services measures. The first one is a study on the impact of the FSAP[103]. The second one is on the cost of compliance with selected FSAP measures, notably including the AML Directive. This second study is largely based on individual interviews with credit and financial institutions, including around 40 banks and financial conglomerates and 18 investment banks.

Other publicly available information has been used for the preparation of this document, such as publications from: the Commission and advisory bodies to the Commission; national supervisors; the Basel Committee of Banking Supervision and similar international bodies; the FATF; financial services industry; leading international consultancy firms etc (see below list of References for further detail).

[102] The Article 29 Data Protection Working Party was created by Article 29 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. See http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

[103] See http://ec.europa.eu/internal_market/finances/actionplan/index_en.htm .

ANNEX 3 – SUPERVISION ON AML COMPLIANCE BY BANKING INSTITUTIONS IN THE EU

A) Supervisory expectations on global risk management by banks

Global risk management, including AML risk, by banks is a clear supervisory recommendation. For instance, the Basel Committee[104], which is the leading international body in this regard[105], considers that the adoption of effective "know-your-customer" (KYC) standards is an essential part of banks' risk management practices, as banks with inadequate KYC risk management programmes may be subject to significant risks, especially legal and reputational risk[106]. The Basel Committee recognises in this regard that a key challenge in implementing KYC policies and procedures is how to put in place an effective groupwide approach, since those risks are global in nature. As a consequence it underlines that "*it is essential that each group develop a global risk management programme supported by policies that incorporate groupwide KYC standards. Policies and procedures at the branch- or subsidiary-level must be consistent with and supportive of the group KYC standards even where for local or business reasons such policies and procedures are not identical to the group's*"[107].

For the Basel Committee, "Consolidated KYC Risk Management means an established centralised process for coordinating and promulgating policies and procedures on a groupwide basis, as well as robust arrangements for the sharing of information within the group. […] Similar to the approach to consolidated credit, market and operational risks, effective control of consolidated KYC risk requires banks to coordinate their risk management activities on a groupwide basis across the head office and all branches and subsidiaries."[108] The four essential elements of sound KYC programme would be: risk management, customer acceptance policy, procedures for customer identification and process for monitoring its accounts.

The Basel Committee notes that KYC involves in most cases the liabilities rather than the assets side of the balance sheet, as well as balances that are carried as off-balance sheet items. For an appropriate risk management process, the Basel Committee sees it essential, in conducting effective monitoring on a groupwide basis, that "*banks be free to pass information about their liabilities or assets under management, subject to adequate legal protection, back to their head offices or parent banks*"[109]. In this connection, the Basel Committee called on

---

104 The Basel Committee on Banking Supervision is a committee of banking supervisory authorities which was established by the central bank Governors of the G-10 countries in 1975. It is made up of senior representatives of banking supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States. The permanent secretariat is located at the Bank for International Settlements in Basel. See www.bis.org.bcbs.index.htm

105 The International Organisation of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS) have also addressed the money laundering problem. To the extent that this paper is focusing on banking groups, IOSCO and IAIS guidance and recommendations will not be addressed in this paper. For a summary view of IOSCO and IAIS work in the AML field, see the Joint Forum (2005).

106 Basel Committee (2004).

107 *Ibid*. §3.

108 *Ibid*. §4.

109 *Ibid*. §5.

jurisdictions to facilitate consolidated KYC risk management by providing an appropriate legal framework which allows the cross-border sharing of information.[110]

B) Non-transparent jurisdictions and the "know-your-structure" principle

Particular challenges regarding global AML risk management appear in connection with the activities of subsidiaries and branches of credit institutions in jurisdictions which lack or impair transparency[111]. Operating in such jurisdictions, particularly when performing certain services or establishing opaque structures on behalf of customers, pose financial, legal and reputational risks to the banking organisation, impede the ability of the board of directors and senior management to conduct appropriate business oversight and hinder effective banking supervision.[112] These non-transparent jurisdictions furthermore constitute a threat to the stability and reputation of the financial system as a whole. In its declaration of 15 November 2008 the Group of Twenty (G-20), in order to promote integrity in financial markets, called on national and regional authorities to implement national and international measures to "*protect the global financial system from uncooperative and non-transparent jurisdictions that pose risks of illicit financial activity*".[113] In a recent communication, the Commission suggested that "*a list of uncooperative jurisdictions should be drawn up together with a toolbox of joint measures for use against them in the areas of supervision, anti-money laundering, terrorist financing and taxation*". It further suggested that banks should be dissuaded from operating in off-shore centres through increased prudential requirements and tougher transparency rules[114]. The Group of Twenty, in April 2009, further stated that "*it is essential to protect public finances and international standards against the risks posed by non-cooperative jurisdictions*" and called on all jurisdictions "*to adhere to the international standards in the prudential, tax and AML/CFT areas*"[115]. The Group of Twenty also agreed that the FATF should revise and reinvigorate the review process for assessing compliance by jurisdictions with AML/CFT standards.

In this connection, the Basel Committee has stressed the importance of the "know-your-structure" principle in the banking sector with a view to mitigate the risks arising from the activities of banks in non-transparent jurisdictions which potentially impede effective supervision[116]. It first recommends that the board and senior management should understand the bank's operational structure, particularly where the bank operates in jurisdictions that impede transparency.

The Basel Committee further recommends that the board of directors and senior management should conduct an enhanced level of due diligence where a bank operates in jurisdictions that reduce transparency and potentially impede effective supervision. In this regard, it recommends that banks should have appropriate policies and procedures in place, *inter alia*, to: regularly evaluate the need to operate in jurisdictions that reduce transparency; identify and manage all material risks, including legal and reputational risks, arising from such

---

110 *Ibid*. §6.

111 This could include offshore financial centres and onshore jurisdictions in which a lack of transparency and weak enforcement mechanisms foster opacity and hinder effective management and supervision. It is assumed that those non-transparent jurisdictions are outside the EU.

112 Basel Committee (2006), §52, 53.

113 Group of Twenty (2008)

114 European Commission (2009), p.17.

115 Group of Twenty (2009b).

116 Basel Committee (2006), §§ 52 to 56 (Principle 8)

activities; set forth clear corporate governance expectations and responsibilities for all relevant entities and business lines within the banking organisation; oversee the regular assessment of compliance with all applicable laws and regulations, as well as the bank's own internal policies; ensure that these activities are within the scope of regular head office internal controls, as well as external audit reviews; or ensure that information regarding these activities and associated risks is readily available to the bank's head office and is appropriately reported to the board of directors and supervisors.[117]

The know-your-structure principle has been – to some extent – included, for banking institutions, in the EU directive relating to the taking up and pursuit of the business of credit institutions[118].

C) The notion of group in the Directive: beyond the "know-your-structure" principle

The notion of group is, however, not foreign to the AML Directive, on the contrary. In the first place, Article 34(2) integrates the "know-your-structure" principle by requiring credit and financial institutions covered by the Directive to communicate to their branches and majority owned subsidiaries located in third countries (irrespective of whether these jurisdictions impede or reduce transparency) their relevant internal policies and procedures in this area. These policies and procedures should relate[119] to "*customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing*". Additionally, this principle is further developed in Article 31(1) which requires credit and financial institutions covered by the Directive to apply in their branches and majority owned subsidiaries located in third countries, measures at least equivalent to those laid down in the EU AML Directive with regard to customer due diligence and record keeping. This second requirement results in a *de facto* "exportation" of the EU rules, indeed beyond the "know-your-structure" principle.

Although the obligations in Articles 31(1) and 34(2) of the Directive only concern subsidiaries and branches in third countries, the logic behind both articles is that risk management and AML compliance is conducted at group level irrespective of where the subsidiaries or branches are located. Indeed, the Directive implicitly integrates the logic of compliance at group level also for subsidiaries and branches located within the EU. It contains no explicit rules on this, but the principle can be inferred from the rules on the sharing of information regarding money laundering suspicions reported to the financial intelligence units. Article 28(3) of the Directive waives the tipping-off prohibition in order to allow for information sharing within credit and financial institutions belonging to the same group of

---

117 *Ibid*. §56. Regarding particularly the question of internal controls, the Basel Committee states that "*[t]he board and senior management can enhance their effectiveness by requiring that internal control reviews include not only "core" banking businesses, but also activities conducted in jurisdictions […] that lack transparency. These reviews should include, for instance, regular inspection visits by internal auditors, review of activities to ensure that they are in line with their initial intended purpose, review of compliance with applicable laws and regulations, and assessment of legal and reputational risks arising from those activities or structures. […] and management should ensure that the board is notified of the existence and management of any significant risks that are identified.*", *Ibid*. §55.

118 See Articles 73(3) and 22 as well as Annex V 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 (recast), OJ L 177, 30.6.2006, p.1.

119 Cf. Article 34(1).

companies[120]. It is implicit in this Article that such sharing of information within the group is needed in order to apply a consolidated risk (including AML risk) management policy at group level. In this context, Article 28(3) of the Directive provides a definition of group of credit and financial institutions for the purpose of sharing information, which one could extrapolate for any application of the principle of compliance at group level across the Directive. This definition is by reference to Article 2(12) of Directive 2002/87/EC:[121] "'*group shall mean a group of undertakings, which consist of a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 12(1) of Directive 83/349/EEC*".[122]

D) Supervision of AML compliance in the EU: consolidated or concurrent

The AML Directive requires that national competent authorities supervise compliance of credit and financial institutions with the requirements of this Directive and that competent authorities are granted adequate powers and resources in this regard[123]. Almost all banking supervisory authorities (CEBS members) in the EU have been given the objectives (solely or as a shared responsibility) of protecting banks' clients from misconduct and/or bad business practices and of preventing financial crime, including anti-money laundering[124]. However not all of them have the power to monitor compliance with the AML Directive: twenty-one banking authorities (AT, BE, BG, CY, CZ, DE, EE, EL, FI, FR, HU, IE, LV, LU, MT, NL, PT, RO, SE, SI and UK) possess this power while two authorities (DK, ES) do not and four (IT, LT, PL and SK) do not possess it fully[125].

Supervision of AML compliance in the EU: organisational structure

120 "*3. The prohibition laid down in paragraph 1 shall not prevent disclosure between institutions from Member States, or from third countries provided that they meet the conditions laid down in Article 11(1), belonging to the same group […]*."

121 Directive 200/87/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; OJ L 35, 11.2.2003, p.1. Consolidated text available at: www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0087:20050413:EN:PDF

122 The seventh Company Law Directive on consolidated accounts. Article 12(1) of this Directive states: "*1. Without prejudice to Articles 1 to 10, a Member State may require any undertaking governed by its national law to draw up consolidated accounts and a consolidated annual report if: (a) that undertaking and one or more other undertakings with which it is not connected, as described in Article 1(1) and (2), are managed on a unified basis pursuant to a contract concluded with that undertaking or provisions in the memorandum or articles of association of those undertakings; or (b) the administrative, management or supervisory bodies of that undertaking and of one or more other undertakings with which it is not connected, as described in Article 1(1) or (2), consists for the major part of the same persons in office during the financial year and until the consolidated accounts are drawn up.*"
Consolidated text available at:
www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1983L0349:20070101:EN:PDF

123 Cf. Article 37.

124 CEBS (2009), §39 and seq.. Only in ES this is not the case: the AML supervisor is the FIU, which is administratively attached to the banking supervisor (*ibid*, §43).

125 In many cases (ES, LU, MT, PL and SK) the FIU is also a competent authority in respect of monitoring compliance with the AML Directive and in IT the Financial and Economic Police possess this power. In MT, the banking supervisor powers regarding AML are delegated by the FIU. See CEBS (2009), §173 (references regarding DE, FI, MT, RO, SE and SK have been updated on the basis of information provided by national authorities).

There are different models across the EU for the supervision of credit and financial institutions. For instance, in AT, BE, BG, EE, HU, IE, FI, LV, SE, SK and the UK there is one supervisory authority which covers all or most credit institutions as well as the prudential and market conduct supervision, including the supervision on AML. In other Member States such as CY, EL, FR, IT, LT, LU and RO one can identify a sectoral division and/or a division of tasks based on prudential vs. market conduct supervision. If there is a sectoral division, then the AML responsibility lies with the supervisor responsible for the respective sector. Where there is a division based on prudential vs. market conduct supervision, the responsibility for AML lies in most cases with the prudential supervisor.

Nevertheless, there are exceptions to this principle. An example of such exception is DE where the central bank (*Bundesbank*) assists the financial supervisory authority (*BaFin*) in the prudential banking supervision, while *BaFin* is an integrated supervisory authority covering all credit and financial institutions with regard to prudential and market conduct supervision. Featuring a cross-sectoral AML group, *BaFin* has the exclusive responsibility for the AML supervision of the financial sector. Another exception is NL where a combination exists of a sectoral division and a division in prudential vs. market conduct. The supervision regarding AML lies with the supervisor who has the licensing authority for a credit and financial institution. In ES, a dedicated commission for the prevention of money laundering has been set up. This commission has two supporting bodies, namely a secretariat and the executive office, the latter acting as both the Spanish FIU and as AML supervisor. Having said this, the Spanish prudential supervisors will focus on reviewing the "know-your-customer" (KYC) prudential standards and report their findings to the executive service of the dedicated commission. In BG, besides the Central Bank the the Financial Supervision Commission, AML supervision in the banking and financial sector is conducted by the FIU as well.

Source: CEBS and information provided by national authorities.

The Directive, however, does not set up rules regarding the supervision of groups with institutions established in more than one Member States. As a result, in all Member States, locally established subsidiaries or branches of credit and financial institutions from other Member States (as well as from third countries) are subject to local AML supervision like the local credit and financial institutions[126]. At the same time, despite the absence of a clear framework in the AML Directive regarding supervision on AML compliance by groups, in almost all Member States (if not all), AML supervision carried out by the supervisory authority of the parent institution encompasses the branches and subsidiaries[127] located in other EU Member States. In some Member States, such as FR or DE, this is an explicit legal requirement, while in other Member States, such as IE, it is the result of supervisory guidance. In other Member States, such as BE, EL, NL or the UK, the focus of the supervisory authority is on the head office and its senior management responsible for ensuring that their foreign branches and subsidiaries are complying with the group AML standard. The obvious result is that more than one national supervisor may intervene for the same group in different countries, thus making duplications (and potentially divergences) possible.

Additionally, competent supervisors for AML issues may have different nature: in a few instances they are not the same as those tasked with "prudential" supervision (see also

126 Some Member States, such as BE, may however address differently branches and subsidiaries from non-EU credit and financial institutions compared to branches and subsidiaries from EU institutions. In the second case, AML supervision would be more specialised and focused and not integrated with prudential supervision (to be conducted by the Home Member State)

127 This does not imply that the supervisor of the parent institution will be able to directly impose enforceable requirements on its subsidiaries abroad.

above)[128]. According to CEBS, twenty-one EU banking supervisors have the power to carry out AML supervision also on a consolidated basis for banks[129].

How the supervision is integrated into the supervisory approach?

In several Member States, such as AT, BE, FR, IE, LT, LU, PT, SK and RO, the AML supervision is integrated into prudential supervision. In other Member States, such as BG, CY, EL, FI, HU, LV, NL and SE, the AML supervision forms part of the prudential supervision, but is also performed as a separate supervisory task. As a result thereof, specific on-site visits concerning AML may be planned separately. In ES, the supervision of KYC prudential standards is performed by the sectoral supervisors, while AML supervision is performed by the specialised AML supervisor. In IT, while sectoral supervision have the competence to conduct general AML supervision, the FIU performs checks on compliance with the obligation to report suspicions.

For instance, in BG, CY, EL, FR, HU, LU, LV, NL and SE specific arrangements in place for AML supervision may include: dedicated competent departments; specific planning and separate on-site inspections; as well as, in some cases, the requirement that the annual risk assessment of supervised institutions include observations relating to AML issues.

Source: CEBS and information provided by national authorities.

This complexity also appears in the Basel Committee recommendations in this regard. For the Basel Committee, in a cross-border context, home country supervisors should face no impediments (in particular by local bank secrecy laws) in verifying a branch or subsidiary's compliance with groupwide KYC polices and procedures during on-site inspections. The Basel Committee also underlines that the host country supervisor retains responsibility for the supervision of compliance with local KYC regulations (which would include an evaluation of the appropriateness of the procedures)[130]. In order to overcome this complexity, the Basel Committee recommends two lines of action:[131] firstly, supervisors should ensure that there is appropriate internal reporting and communication from the branch/subsidiary to the board of the parent bank, and viceversa, in respect of all material risk and other issues which may affect the group (e.g. groupwide "know-your-structure"); and secondly, banking supervisors should cooperate and share information with other supervisors to enhance supervisory effectiveness and reduce supervisory burden.

Supervisory authorities in the EU have also addressed this problem. On the one hand, they have arrangements and practices in place for cooperation and exchange of information among them[132]. The exchange of information is permitted in many (but not in all) cases, but restricted

128 On this issue, see generally de Larosière Group (2009), in particular annex III to that report.

129 AT, BE, BG, CY, DE, EE, EL, FI, FR, HU, IE, LU, LV, MT, NL, PL, PT, RO, SE, SI and UK. On the contrary, DK, ES and LT do not have the power and CZ, IT and SK share the power with the FIU. See CEBS (2009), §176 (references regarding FI and SK has been updated on the basis of information provided by national authorities).

130 Basel Committee (2004), §21.

131 Basel Committee (2006), §63.

132 According to CEBS, of the EU banking supervisors, eighteen authorities (AT, BE, CY, CZ, DE, EE, EL, FI, FR, IT, LT, LV, NL, PT, RO, SE, SI and UK) have the power of cooperating and exchanging information with foreign authorities tasked with AML. Nevertheless BE and RO indicated that they will share information with foreign supervisors, i.e. for purposes of conducting their supervisory role and AT mentioned that it is bound by law with certain restrictions. Parallel with the cooperation and exchange of information on a national basis, DK, ES and MT do not have this power internationally (in MT, the power lies with the FIU). In addition, several authorities (BG, HU, IE, LU, PL and SK) do not fully possess the power to cooperate and exchange information with foreign authorities tasked with

to when it fits the purpose of the assignment and provided it is kept confidential. Arrangements are not necessarily AML specific but through different prudential instruments. On the other hand, notwithstanding the way the supervision is structured, many Member States supervisory authorities have conducted on-site visits to other EU countries (and beyond). This supervisory cooperation within the EU has been reinforced by the creation of a dedicated anti-money laundering task force by the so-called level 3 committees (CEBS, CESR and CEIOPS)[133].

Specific tools used for AML supervision

Various tools are used across Member States for supervision in the AML area. As required by the AML Directive (cf. Article 37(3)), all Member States supervisory authorities perform on-site inspections with respect to AML. Some of them (such as BG, CY, EE, EL, FI, UK) have adopted a risk based approach to supervision, which implies that all firms are subject to a "baseline monitoring" and that the nature and intensity of a supervisory's relationship depends on the assessment performed by the supervisor. The purpose of the inspections is to determine the compliance with legislation regulating the prevention of money laundering; assessing the effectiveness of the internal control systems concerning customer identification procedures; risk management; the KYC principle; monitoring and reporting of suspicious transactions; record keeping and staff training. These on-site visits may form part of regular on-site inspections, have a specific integrity scope or form a follow up to specific cases. In some Member States, such as BG, DE, FI, FR, IE, NL, PT, SE and the UK thematic AML inspections are also being conducted. Almost all authorities have issued internal manuals for prudential supervisors' use for on-site inspections. A special section in these manuals is specific to AML. Otherwise, detailed checklists or questionnaires are also being used to guide examiners.

Aside from on-site visits, most Member States supervisory authorities also use additional off-site tools. In Member States such as CY, EL and LU the annual activity report drawn up by the designated money laundering officer has to be sent to the supervisory authority and, as the case may be, also to the company's auditor. In AT and DE, the supervisory authority receives a certified annual report and in FR and SK an internal control report with information on AML. In FR, banks should also fill in a questionnaire prepared by the supervisor allowing to have a detailed description of the AML framework of the banks concerned. In ES, regulations require banks to present independent expert reports annually. Other examples of off-site tools are: (annual) questionnaires, self assessments, statistics, training programmes and a web tool which serves as a comparison of compliance and awareness between different types of institutions. In addition, in some Member States (such as BG, EL, FI, FR) regulation requires that credit institutions must check the compliance of a new products[134] to AML requirements before they can validate it. Finally, supervisors may receive from credit institutions copy of part or all AML related information those institutions disclose to FIUs or public prosecutors.

Generally, supervisory authorities provide their staff with specific training on AML issues.

Source: CEBS and information provided by national authorities.

E) Supervision of AML compliance in connection to non-cooperative jurisdiction

AML. See CEBS (2009), §178 (references regarding CZ and FI have been updated on the basis of information provided by national authorities).

133 For further information on CEBS, CESR and CEIOPS, see Annex 2.
Concerning the level 3 committees' architecture, see the recent reflection undertaken by the de Larosière Group. In its vision for the future, this group proposes a new structure for the cooperation of national supervisors with increased powers at European level regarding prudential supervision. Interestingly, the group foresees that AML supervisory task will remain national. See de Larosière Group (2009), p.42 and seq., and annex V.

134 In the case of BG, regarding products that may favour anonymity.

Additionally, where banks operate in **jurisdictions that impede transparency**, the Basel Committee suggests that "*countries should work to adopt laws and regulations enabling bank supervisors to obtain and review the documentation of a bank's analysis and authorisation process and to take appropriate supervisory action to address deficiencies and inappropriate activities when necessary*".[135] This line of reasoning is also integrated in the AML Directive. Article 31(1) second paragraph states that where the legislation of a third country does not permit application of measures equivalent to those laid down in the Directive with regard to customer due diligence and record keeping by the subsidiaries and branches of EU credit and financial institutions, the EU institution concerned shall be required by national law to inform the competent authorities of the relevant home[136] Member State accordingly[137]. The Directive does not impose a particular task to supervisors in this regard, but rather to credit and financial institutions themselves which, in accordance with Article 31(3) shall be required to take additional measures to effectively handle the risk of money laundering or terrorist financing deriving from its activities in this type of third countries. The Directive is not explicit as to whom should require credit and financial institutions to take those additional measures, but this task seems to be devoted in practice to the supervisor. In any event, the intervention of the supervisor would be allowed by the general provision on supervision contained in Article 37.[138]

Recent policy developments at EU and international level are addressing the non-cooperative jurisdiction issue (see above part B of this Annex)[139].

---

135 Basel Committee (2006), §63.

136 The reference to the home Member State should possibly be interpreted as referring to the State of the ultimate parent company of the financial group. Otherwise, this would lead to concurrent supervision of compliance with Article 31 if the subsidiary in a third country is itself a subsidiary located in one MS of a parent company located in another MS.

137 In addition to this information duty, national legislation may be more prescriptive. For instance, a recent German law foresees that a parent institution domiciled in DE must also ensure that a subordinated enterprise, a branch or subsidiary in a non-cooperative jurisdiction does not establish or continue business relationships and does not undertake transactions if the obligations for the parent institution are impermissible or not actually practicable in a State where the subordinated enterprise is domiciled. Insofar as a business relationship already exists, the superordinated enterprise or parent enterprise must ensure (with means under company law) that such relationship is terminated by giving notice of termination or by other means by the subordinated enterprise, the branch or the subsidiary regardless of other legal or contractual provisions (cf. Section 25g of the Banking Act).

138 According to anecdotal data collected by the Commission services, in at least 2 Member States (FR and PT) the supervisory authorities have been informed by banks of problems in applying CDD and record keeping measures in third countries.

139 See also, regarding financial regulation and prudential supervision, the recommendation recently made by the de Laroisère Group on poorly regulated or uncooperative jurisdictions, de Larosière Group (2009), p.65 and seq.

ANNEX 4 – THE INTERNAL ORGANISATION FOR AML COMPLIANCE

Banks with branches and subsidiaries outside their Member State of establishment (whether in the EU or outside the EU) are generally organised to manage compliance risk[140] as a group, that is: ensuring that the business complies with existing legislation and regulation, as well as with internal policies and ethical standards. This includes compliance with AML legislation within the EU. Indeed, a recent study conducted for the Commission indicates that trans-national banks (and asset managers) have typically implemented the AML Directive provisions on a group basis[141]. This is consistent with the general belief that global risk management is more efficient[142]: through a centralized system, the flow of information allows the central compliance department to respond faster and more efficiently in case of suspicious of money laundering; the know-how of the parent company can be gradually integrated in their subsidiaries; and economies of scale can be achieved.

A) The growing importance of the compliance function

This compliance activity is increasingly integrated in the so-called 'compliance function'[143]. The compliance function is generally seen as having an important role to play in the mitigation of reputational risk for the institution[144]. Indeed some research found that non-compliance with legal obligations is seen as the most significant source of reputational risk for businesses[145]. Also, a study conducted for the Commission found that most of the banks and financial conglomerates participating in the survey ranked adapting to or anticipating to regulatory change (regardless of the source) as the most important driver of compliance strategy[146].

---

140 The Basel Committee defines 'compliance risk' as the "*risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities*." See Basel Committee (2005), §3.

141 Europe Economics (2009), §4.62. These findings are consistent with those of a global survey undertaken by a consultancy firm in 2007. In this survey, 94% of internationally active banks responding to the survey from the European region reported that they had a global AML policy in place. 49% of those stated that they had a full global approach (i.e. AML policies and procedures are developed at global level and implemented as consistently as possible worldwide) and 45% reported that they had a hybrid approach (i.e. there is a global AML policy but detailed procedures are set at a regional/local level). Only 6% would have a full AML local approach. According to this survey, "*European banks were significantly more likely than those in other regions to apply a global approach, reflecting the high-level and flexible nature of much European AML legislation*." See KPMG (2007), pp.19 and 52.

142 Implicit in Basel Committee (2004) and Basel Committee (2005) as regards supervisory expectations. Also, information collected by the Commission services from major audit firms supports this opinion.

143 The Basel Committee uses the expression 'compliance function' to describe staff carrying out compliance responsibilities, without intending to prescribe a particular organisation structure. See Basel Committee on Banking Supervision (April 2005), *Compliance and the compliance function in banks*, §5.

144 Therefore, one could also assume that some compliance activity is likely to occur in the absence of regulation. See Europe Economics (2009), §3.5.

145 See Economist Intelligence Unit (2005), *Reputation: risk of risks*. This study surveyed 269 senior executives, of which 36% were drawn from financial services sector companies. See also KPMG (2007) which suggests that, in general, concerns about the potential reputational damage of inadequate AML policies and procedures has led most banks to adopt global minimum standards (p.19).

146 Europe Economics (2009), §3.10 and seq.

In this context, the importance of the compliance function within banks has particularly grown in recent years and is becoming part of the firms' culture. Drivers of this growth include increased regulatory expectations for specific operational compliance activities (notably including AML[147]) and the switching of resources from internal audit to compliance – which in essence, refocuses effort towards prevention rather than treatment[148]. Supervisors are supporting this trend. The Basel Committee has indeed promoted ten basic principles for the compliance function so that the bank will be able to manage its compliance risk more effectively, without necessarily prescribing any particular organisation structure[149]. The respect of these principles has recently been measured by the Basel Committee[150].

Most of the surveyed institutions in the previously mentioned study have an independent, specialised compliance unit within their firm: i.e. it is not an integrated function within a larger department such as the legal or risk management department. Compliance models do vary somewhat across the surveyed firms, but large firms have been able to established compliance functions on a decentralised basis giving a multiple lines of defence structure. The elements within such strategy would variously include the ingrained attitudes of staff (achieved through corporate culture or training), the location of compliance people within individual business units, the centralised compliance function (including a head for the group compliance to whom local compliance officers would report[151]) and internal audit as a final line of defence. Also, the sharing of compliance functions across a number of departments is common to most banks – the compliance unit being responsible for addressing "classic" compliance roles and a risk control function that is responsible for compliance issues relating to, for instance, capital requirements[152]. Recent developments also suggest that having a standalone compliance function may be a significant factor in developing a role that is more proactive than reactive (i.e. it is monitoring activity rather than simply proffering advice) and that has an increasing operational edge.

---

147 See also Basel Committee on Banking Supervision (April 2005), *Compliance and the compliance function in banks*, §4: *"Compliance laws, rules and standards generally cover matters such as observing proper standards of market conduct, managing conflicts of interest, treating customers fairly, and ensuring the suitability of customer advice. They typically include specific areas such as the prevention of money laundering and terrorist financing, […]."*

148 The Basel Committee recommends that the compliance function and the audit function should be separate, to ensure that the activities of the compliance function are subject to independent review. For this, it is important that there is a clear understanding within the bank as to how risk assessment and testing activities are divided between the two functions and that this is documented. See Basel Committee on Banking Supervision (April 2005), *Compliance and the compliance function in banks*, in particular principle 8 (relationship with internal audit).

149 See Basel Committee on Banking Supervision (April 2005), *Compliance and the compliance function in banks*, §6.

150 Basel Committee on Banking Supervision (2008), *Implementation of the compliance principles – a survey*. This survey covered 21 jurisdictions (including 10 EU Member States).

151 The Basel Committee recommends that each bank should have an executive or senior staff member (referred to as 'head of compliance') with overall responsibility for-coordinating the identification and management of the bank's compliance risk and for supervising the activities of other compliance function staff. See Basel Committee on Banking Supervision (April 2005), *Compliance and the compliance function in banks*, in particular principles 5 (independence) and 9 (cross-border issues).

152 Europe Economics (2009), §3.37 and seq. The surveyed institutions, further to banks, financial conglomerates and investment banks, also include asset managers and stock exchanges.

According to this survey, normally the head of compliance would have access to the board either directly or indirectly through the firm's secretary general or the chief counsel. In a small minority of cases the compliance function is directly represented in the executive board[153].

B) The internal organisation: the AML specificities

The internal organisation in banks regarding the prevention of money laundering and the compliance with the AML obligations is normally described as being composed of three lines of defences: the compliance function responsible for the internal policies; the front office/operational staff and the internal/external audit function[154].

i) The compliance function: the MLRO and the internal policies

The compliance function normally integrates compliance with the AML obligations[155]. It is worth highlighting in this context that, according to a study conducted for the Commission, money laundering responsibilities is ranked first by the surveyed banks and financial conglomerates in terms of resource allocation within the compliance function (see chart below)[156]. This reflects the importance of the money laundering risk in a bank's operational model and also the importance attached to AML by senior management[157]. Indeed, there is evidence that senior management in banks are more directly involved in AML activities than previously[158].

---

153 See also Europe Economics (2009) §3.44 and seq. for further detail on the ration of compliance staff to all staff (intensity) as well as on cost control and compliance.

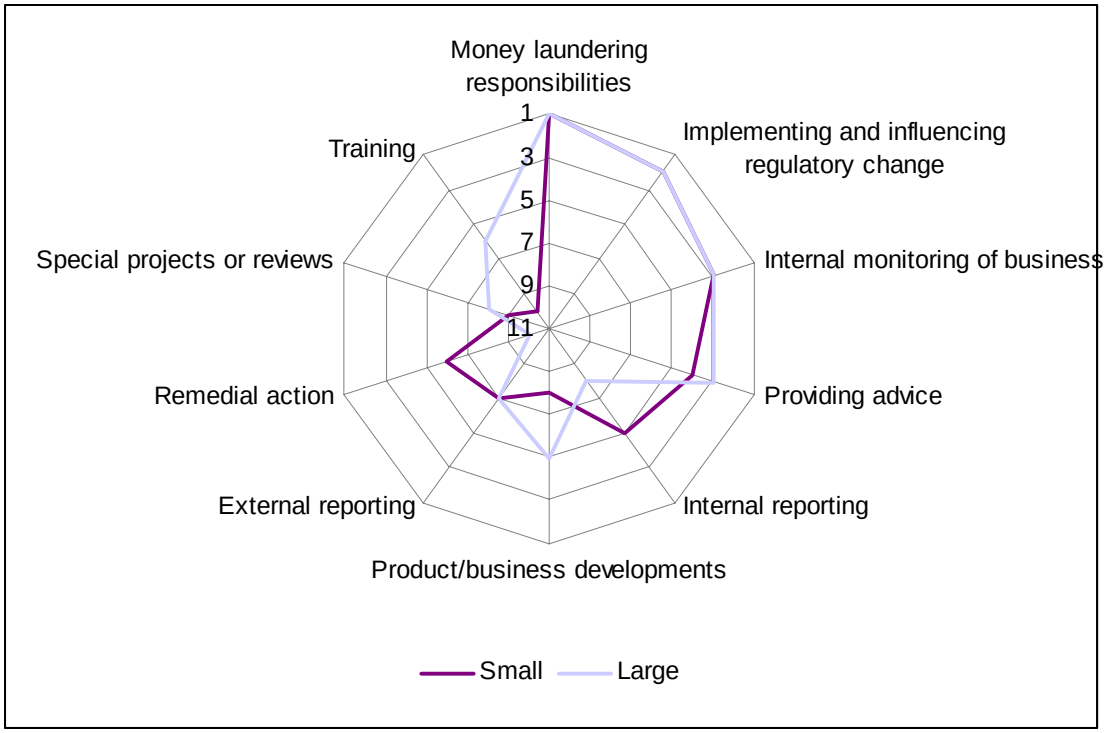
154 KPMG (2007), p.22-23.

155 See Basel Committee on Banking Supervision (2008), *Implementation of the compliance principles – a survey*, §31. According to this survey, the prevention of money laundering and terrorist financing was always mentioned by respondents as being included in the compliance risk. This is confirmed by the study conducted by Europe Economics (2009) and the survey carried out by KPMG (2007).

156 Europe Economics (2009), §3.14 and seq. The investment banks covered in that study also rank the money laundering responsibilities high regarding resources allocation within the compliance function: it comes second after the advising activity (see §3.28 and seq.). Interestingly, for the surveyed asset managers, the money laundering responsibilities have a lower(but still high) degree of importance, which also reflects the fact that they are not in the front line of the AML defences as banks are (see §3.22 and seq.).

157 According to an independent global survey carried out by a consultancy firm in 2007, "*AML remains a high profile issue for the senior management of banks globally*". In this survey, 70% of European banks reported that their most senior levels of management – including their board of directors – take an active interest in AML compliance, while a further 29% of the European banks stated that senior management took 'some interest' in AML issues. For this firm, "*the increased profile of AML as an issue is part of the broader shift in the governance of world's major banks, with boards of directors being held more directly accountable by shareholders and regulators for the full range of risk run by their banks*." See KPMG (2007), p.11. A similar survey, though limited to the UK, also outlines the senior management engagement in AML issues was high. See PWC (2007b), p.7.

158 CRA International (2009), p.13 and section 3.7.3. See also FSA (2008), p.12.



Source: Europe Economics (2009).

The central role for AML within banks' organisation is with the anti-money laundering officer[159]. In most countries, the existence of a MLRO is compulsory by law[160]. The MLRO will normally hold a high position in the firm and integrate in the compliance function, but the MLRO will not necessarily be the head of compliance. He/she will typically report to the board, either directly or indirectly through another senior official[161]. For instance, in UK firms, where the role of MLRO is well established, he/she will normally prepare an annual report addressed to the company board. In large firms, a broadly common approach is that he/she produces a monthly report to the compliance directors, covering, amongst other things, major fraud or money laundering incidents or cases[162]; the status of AML related projects; and the status of action taken in response to recommendations raised in the previous year's MLRO annual report to the board[163].

In the case of groups, MLROs will be appointed in each jurisdiction where the group is present, if so required – which is usual – by national legislation[164]. Nevertheless, group

159 Generally referred to as money laundering reporting officer (MLRO) or money laundering compliance officer (MLCO).

160 For instance, this is the case in at least: AT, BG, DE, EE, EL, FR, LU, MT, PL, SE, SI, SK, UK.

161 *Mutatis mutandis*, see High-Level Group on Financial Supervision in the EU – chaired by Jacques de Larosière (2009), p. 32 on the importance of (general) risk management, the need for independence of the risk management function and the need for direct access to the board of the senior risk officer (who should hold a very high rank in the hierarchy).

162 In many cases, banks' departments dealing with the money laundering risk, will typically deal with the fraud risk as well. See KPMG (2007) p.22. Regarding UK banks, the creation of a financial crime unit (with potential to also encompass market abuse) appears to be a supervisory expectation. See PWC (2007b), pp.8 and 9and FSA (2008), p.15. On fraud issues, see generally, PWC (2007a).

163 FSA (2008), p.13

164 Even if not required, in practice banks prefer to have a local MLRO or at least a local "satellite" of the MLRO, who will ac as the key contact for the regulator.

compliance officers are typically (but not always) appointed at group level for the internal control and compliance management[165].

For EU banks, the practice is that head office establishes the internal policies and procedures that all the subsidiaries and branches in other EU countries (and in third countries) must implement (without prejudice to the compliance with local rules). This is consistent with the supervisory expectation[166] and with national legislation implementing the AML Directive (as regards third countries)[167]. In doing so, anecdotal evidence suggests that many larger institutions apply the "higher of home or host" rule to their AML policies and procedures, but recognising that particular local nuances in applicable laws, including data protection legislation, must be considered[168]. Staff of the parent bank periodically revises the implementation of these policies and procedures and test the effectiveness of controls. This may include visits to the countries concerned.

Some views have been made[169] anticipating that a major challenge for EU banks will be to use the greater flexibility offered by the risk based approach in the Directive while at the same time leaving a sufficient audit trail for the process whereby they have made decisions about the key AML risks and the suitability of controls to mitigate these risks. Documenting this process is particularly important when rules and supervisory expectations differ from country to country. Another identified challenge is the effective implementation of policies and procedures rather than their initial design: e.g. clarity of the policies for employees, training and communicating the policies and procedures, and the application of these including monitoring effectiveness on a regular basis[170]. The supervisory expectation is that the compliance function and the audit function (see below) take on this effectiveness evaluation task[171].

ii) Front office and operations staff: automation and training

Vigilant front office and operations staff are key to banks' AML policy regarding customer acceptance and on-going monitoring for the identification of suspicious activity. Their role is supplemented by sophisticated IT solutions (such as IT monitoring systems) which are increasingly used by banks (in particular large banks) for AML compliance. It is indeed reported that IT solutions are seen as (more or less) necessary to fulfil some compliance

---

165 In AT, for instance, it is not possible to appoint a MLRO without the permission of the supervisor.

166 See Basel Committee (2004), §8.

167 The Directive requirements concerning the communication of policies and procedures to branches and subsidiaries (cf. Article 34) apply only with regard to third countries, not within the EU. In practice, it is also applied within the EU.

168 Information collected by the Commission services from major audit firms. For global firms, the US or UK requirements are widely used as core standards, but with more detailed policies and procedures at local level reflecting local law.

169 KPMG (2007), p.54.

170 KPMG (2007), p.20. A different survey conducted on UK financial services businesses (not limited to banks) reported that almost all of the firms surveyed had already documented the identified risks. It also underlined the need for enhancing policies and procedures in relation to automation and transaction monitoring, staff training, better systems/computer software and certified/electronic IDs. See PWC (2007b), pp. 5 and 6.

171 See Basel Committee (2004), §9 states that: *"[…] Banks' compliance and internal audit staffs, or external auditors, should evaluate adherence to all aspects of their group's standards for KYC, including the effectiveness of centralised KYC functions […]*".

activities[172] and some firms (generally larger banks) see automation as the only way to provide the necessary evidence of an audit trail to the regulatory authorities in the event of problems arising (as well as being cost effective by comparison to manual effort). At the same time, the design, configuration and management of these IT solutions needs to be carefully considered, notably in the case of larger cross-border institutions, as the risk of false positives is high[173]. In any event, human oversight in this area is still significant[174].

Adequate AML training (as well as awareness) of staff is particularly necessary is the bank wants to be able to play an effective role in preventing money laundering. Banks continue to report that properly trained staff is the best AML control and this is reflected in the continued high spending on training programmes in this field[175]. Another recent survey confirmed that indeed AML training (including also combating terrorist financing and the monitoring of financial sanctions lists) is one of the most common areas for compliance training[176]. This survey also reports that investment in training is seen as a long-term route to savings, by instilling an improved corporate culture: in other words, well-trained staff is expected to ensure that compliance procedures are adhered to during day-to-day activities, reducing the requirement for intervention from the compliance department.

Concerning training methods used, there seems to be a trend towards computer based training or e-learning[177]. This has the advantage of being an important route to cost reduction, but it is also seen as a "quick fix" that requires additional classroom-based training support[178]. Indeed, face-to-face training is largely considered to be the most effective training method[179]. Similarly to the internal policies, the challenge is to make sure that the training delivered is effective and that this results in staff being sufficiently AML aware and capable[180].

---

172 Europe Economics (2009), §3.49. In another survey conducted in 2007 among UK financial services firms, it is reported that there could be synergies between monitoring for suspicious activities by the customers of the credit and financial institutions and suspicious transaction reporting required under the Market Abuse Directive. However, in a significant number of cases UK MLROs were not involved in the consideration of potentially abusive transactions as per the Market Abuse Directive. See PWC (2007b), p.9 and 13.

173 In a survey conducted among UK financial services firms in 2007, the rate of false positives was significantly high, reaching 90% of false positives for about 80% of the respondents. See PWC (2007b), p.10.

174 *Ibid*. §5.40. Also confirmed by KPMG (2007), p.33.

175 According to the KPMG survey of 2007, in 38% of the surveyed European banks, more than 80% of the staff has received AML training in the past two years; in 30% of the banks it was between 60% and 80% of staff, in 21% of the banks, between 41 and 60% of staff and in the rest of the banks, less than 40% of staff. According to this survey, this reflects a risk-based approach to training, which is provided to those with a real need for it. See KPMG (2007), p.39 and seq.

176 Europe Economics (2009), §3.49.

177 Europe Economics (2009), §3.49; KP¨MG (2007), p.40. According to the FSA, in the UK most large firms used some sort of computer based training (CBT) to train staff in AML and other financial crime topics, with refresher trainings having to be undertaken annually. The standard CBT packages included a test which staff were required to pass and the questions of topics covered could also be tailored to suit the business. In addition to this, many firms provided specific training sessions for staff working in certain roles or business areas. See FSA (2008), p. 23.

178 Europe Economics (2009), §3.49.

179 See KPMG (2007), p.40-41. This survey also reports about the most commonly used training methods (such as face-to-face training, computer-based training, written materials, video etc).

180 For instance, in the UK the Joint Money Laundering Steering Group Guidance states that banks should not only obtain acknowledgement from the individuals that they have received the necessary training, but should also take steps to assess its effectiveness. See JMLSG (2007), §7.38. See also KPMG (2007), p.42 and 53. Respondents to another survey conducted in the UK identified training, alongside

iii) Internal and external audit

The third leg in the organisation is the internal or external audit function which provides for independent review and test controls after the event[181]. A 2007 survey[182] showed that independent monitoring and testing of AML systems and controls is increasing[183], though not necessarily under the responsibility of the audit function only[184]. Indeed, in recent times banks seemed to have switched resources from internal audit to compliance – which in essence, refocuses effort towards prevention rather than treatment[185].

Different national laws foresee a particular role for the external audit on the application of the AML obligations by banks[186]. For instance, in Belgium, Germany or Portugal the law requires banks' external auditors to report on their AML systems and controls on an annual basis. In Belgium this report is sent to the supervisor (a similar report should also be sent to the supervisor in Luxembourg). In Greece, audit of internal controls (including AML procedures) is compulsory every 3 years. In Spain, banks must entrust the review of AML procedures to an external auditor with reputable experience and AML knowledge. The report established by this expert is sent to the national FIU/supervisor. In Ireland, it is specifically provided that the auditor needs to gain an understanding of how the bank ensures compliance with the AML legislation. Nevertheless, in many countries there are no auditing standards or standards for banking auditing which integrate standards in relation to the application of the AML obligations by banks. AML obligations are audited under ISA 250 (or similar national standard) which requires the consideration of laws and regulations in an audit of financial statements.

---

technology implementation, as the most important challenges faced by the financial institutions in meeting AML regulations in the future. The survey concludes that "*forward-thinking organisations will take steps to embed the AML regime requirements into key staff consciousness. These efforts will often go beyond a one-off training session. The key to successfully raising staff awareness is to provide support and information on a continual basis.*" The survey also underlines that the culture of an organisation is one of the key components to an effective AML regime. See PWC (2007b), p.11.

181 The Basel Committee recommends that the compliance function and the audit function should be separate, to ensure that the activities of the compliance function are subject to independent review. For this, it is important that there is a clear understanding within the bank as to how risk assessment and testing activities are divided between the two functions and that this is documented. See Basel Committee (2005), in particular principle 8 (relationship with internal audit). See also Basel Committee (2004), §9 on risk management where it is stated that "*[…]. Internationally active banking groups need both an internal audit and a global compliance functions since these are the principle and in some circumstances the only mechanisms for monitoring the application of the bank's global KYC standards and supporting policies and procedures, […]*".

182 KPMG (2007), p.21 and seq.

183 According to the KPMG survey, the vast majority (70%) of the surveyed European banks report that they have a monitoring and testing program in place. However, this survey notes that the European figures (70% of the banks) might need to be adjusted upwards, since the significant low figures provided by German and Swiss banks do not seem to include external auditing reviews but only internal monitoring. *Ibid*., pp.21-22 and 52.

184 The KPMG survey reports that a wide range of functions within banks' organisation are involved in this monitoring and testing, though these functions have different roles and responsibilities in relation to AML. The prevalent role in this regard is with internal audit, compliance function and external audit. Other functions with a role in testing and monitoring the effectiveness of AML systems and controls are: operations, financial crime/fraud prevention units or external consultants. KPMG underlines the increase, compared to 2004, in the amount of AML monitoring carried out by financial crime or fraud prevention units. See KPMG (2007), p.22.

185 Europe Economics (2009), §3.38.

186 It should not be forgotten that auditors are themselves subject to the AML obligations of the Directive.

Concerning the audit of a group, there do not seem to exist specific rules on the split between the auditor at group level and the auditor(s) at subsidiary level. In practice, the group auditor will often wish to instruct the subsidiary auditor in order to obtain a degree of assurance on the AML provisions at subsidiary level. Particular difficulties have already arisen, as shown by anecdotal evidence, regarding access by the head office auditor to subsidiaries' data on reported suspicious transactions to the FIUs. Auditors are considered to be third parties under Article 28 of the AML Directive and therefore are prevented from accessing to such information. Similar difficulties may arise as a result of bank secrecy rules.

When auditors find weaknesses related to the management of the AML risk, they generally report such findings to the Audit Committee or the Board of Directors or both. Management is sometimes also informed and in some instances the auditors at group level are alerted as well.

ANNEX 5 – CUSTOMER DUE DILIGENCE AND REPORTING AT GROUP LEVEL

A) The treatment of the client

Common internal polices on customer due diligence exist within banking groups[187]. Nevertheless, the central application of identification/verification measures to clients and/or customer activity monitoring is not the practice – although banking associations tend to consider that such a possibility would be advantageous[188].

i) The risk based approach to customer due diligence

The existence of those policies does not result either in a uniform application of the internal rules across the group. The AML Directive allows banks to determine the extent of the customer due diligence measures on a risk sensitive basis and, as confirmed by the data obtained by the Commission services, banks are indeed doing so[189]. Different factors are taken into account by banks in implementing the risk based approach, including geographical considerations[190]. This implies that, even if policies and procedures within the group are generally shared, the practical application of the customer due diligence measures will be adapted to local conditions and no box ticking approach followed. Hence, the client of one entity within the group is not automatically accepted as client of all entities of the group.

ii) Customer acceptance policy

Indeed, it appears from the information collected by the Commission services that the parent bank will, in general, not automatically accept customers which have already been accepted by their subsidiaries/branches in other Member States. Branches and subsidiaries abroad will have their own KYC procedures in their jurisdictions and each customer its individual dossier. If necessary, institutions within a group can cooperate to create the dossier but the final result will not be automatically shared and is not used to waive the requirements in another jurisdiction (concerning the flows of information within the group, see part D of this Annex).

---

187 Indeed, the AML Directive requires banks to communicate relevant policies and procedures of customer due diligence to branches and (majority owned) subsidiaries. This is explicitly requested with regard to branches and subsidiaries in third countries (cf. Article 34) and implicitly with regard to branches and subsidiaries within the EU. This is also a supervisory expectation, see Basel (2004), §10 and seq. See also §7 of this paper.

188 Interestingly, the Basel Committee also advanced in 2004 that complementing monitoring of accounts and transactions at local level with aggregated monitoring at the centralised site would provide banks with the opportunity to monitor for patterns of suspicious activity that cannot be observed from the local side. See Basel (2004), §16.

189 See for instance regarding account opening KPMG (2007), p.24 and seq. This survey also notes that roughly three quarters of the European banks have remediation programs in place to 'backfill' customer data regarding customers whose relationship with the bank pre-dates the introduction of current KYC and account-opening legislation. *Ibid*., p.26-27 and p.52.

190 The FATF has recently provided general guidance to the banking industry in this regard. See FATF (2007). In the KPMG survey, the following 5 factors are highlighted by respondent banks at the account-opening phase: the country in which the customer lives or operates; the nature of the customer's business; the type of account or banking product; the anticipated volume and/or value of customer transactions; whether the customer is politically exposed. See KPMG (2007), p.25. See also Basel (2004), §12.

Hence, the parent bank will apply customer due diligence measures, where applicable, not least in order to comply with national requirements which may differ as to the level or detail of customer due diligence measures to be conducted[191] or as to the approaches to information data collection and retention[192]. For instance, concerning the identification of customers and the verification of customers' identities, there are some national constraints to be respected when in cross-border situations. Table A5.1 gives an overview of the types of identification requirements foreseen by national legislation in face-to-face situations[193].

If a customer is transferred within the group, different situations apply to branches and subsidiaries located in the EU. In the case of a branch's customer, a bank may in principle rely in the on already existing identification data held by the branch provided it is up-to-date and fulfils the requirements set out in the destination Member State legislation. This is so because the branch is the same legal person as the bank, therefore rights and obligations are caused by the bank itself. In the case of subsidiaries in the EU[194], normal rules on relations with third parties will be applied. In several Member States, legislation allows (or does not forbid) banks to use agents or third parties (outsourcing) for the identification/verification of customers[195], so a subsidiary could benefit from these provisions. The Directive rules on reliance are also applied in most Member States[196]. These rules allow the bank to rely on the identification/verification of customers already conducted by a third party (in this case the subsidiary[197]). In some cases, legislation has made explicit that the third party should have identified the customer face-to-face, so as to avoid distance identifications or chains of third parties[198], of the fact that third parties should always carry out new diligence measures on the customer concerned without relying on measures previously carried out with those customers[199]. No specific provisions foreseeing a special treatment for customers introduced subsidiaries have been enacted by national legislation – though the application of the risk based approach and the information flows within the group could facilitate the customer acceptance process.

iii) Customer acceptance policy: special cases

---

191 For instance, it is possible that the level/detail of CDD requirements is higher in Member State A (e.g. the country where the customer will be transferred) compared to Member State B (the country of the first identification: e.g. enhanced CDD in Member State A but not in B; or simplified CDD in Member State B but not in A. On this issue, see Part B of this Annex containing information on the different requirements applied by Member States.

192 This is also recognised by Basel (2004), §13.

193 It should be noted that some items may not be directly required by law, but will be part of the normal know-your-customer process undertaken by banks on a risk sensitive basis

194 If the subsidiary is located in a third country, it would also benefit from the reliance rules provided that the AML regime in that third country is considered equivalent to that of the Community (cf. Article 16(1)(b) of the AML Directive).

195 This is at least the case in AT, BE, CZ, DE, DK, EE, EL, ES, FI, FR, HU, IE, LT, LU, NL, RO, SE, SI, SK and UK. However, it is not possible in BG and MT (outsourcing).

196 They are at least applied in AT, BE; BG, CY, CZ, DE, DK, EE, EL, ES (draft law), FI, FR, HU, IE, IT, LU, LV, MT, NL, PL (draft law), PT, RO, SE, SI, SK, UK. They are not applied in LT.

197 In some countries (for instance, BG, CZ, EE or SI), the possibility to rely on a third party is limited to certain types of third party, such as banks or financial institutions only. In any event, these categories would normally encompass the subsidiary.

198 For instance, in AT, BE, EE, EL, IT, LT, LV and SI. Concerning BG, CY, CZ, DE, FI, FR, HU, LU, NL, SK and UK it is allowed to rely on a third party introducer who identified the customer in a non-face to face situation provided, in the case of BG, CZ, FR HU and NL, that enhanced CDD is applied. For DE, the situation has to be taken into account when assessing the risk situation of the customer relationship. In ES, IE and PT additional legislation should clarify the situation.

199 For instance, in AT and DE.

Politically exposed persons (PEPs) and sanctions lists are two areas where banks are making an effort to apply a group policy. Banks increasingly establish specific procedures to identify and monitor PEPs on an on going basis, with a view to apply enhanced customer due diligence measures – as mandated by the Directive.[200] Anecdotal views collected by the Commission services suggest that a centralised approach to PEP compliance is desirable for large organisations with cross-border presence, though local requirements must also be followed. One of the main difficulties identified by the banking sector in this regard is the identification of the PEPs themselves, also considering that there is no single definition of PEP at global level (though at EU level, there is a rather harmonised definition). In order to mitigate their risk – and also because of fear of being sanctioned in case of failure, banks tend to rely on commercial lists which they purchase.[201]

It appears that, as a general rule, lists of terrorists, although they can be provided by the parent bank, are applied by each bank according to local rules. However, many banks would voluntarily apply, to the extent permitted by personal data protection legislation, the sanction lists of the countries where they operate in order to mitigate risks[202]. Indeed, a centralised approach to compliance with sanction lists would be recommended by advisory firms to larger banking organisations with a cross-border presence, as this helps ensuring a consistent approach within the group. Difficulties, as underlined by banking associations to the Commission services, are not to be excluded. For instance, electronic lists are considered as non valid against third parties (only paper list published on the official journal of the European Union are legally binding); the multiplicity of lists renders its updating uneasy and at risk; and the quality of the data does not always allow for the identification of the required person which impairs the effectiveness of the control. The resulting legal risks faced by banks are not insignificant.

iv) Monitoring clients' activities and transactions.

Banking associations report that monitoring at level group is only used for subsidiaries and branches within the same jurisdiction. In cross-border situations, the monitoring of customer activity is conducted directly by the institutions at local level, allegedly due to local regulatory requirements[203]. Even if policies and procedures are applied locally, they are normally

---

200 According to an independent survey conducted in 2007, two thirds of the surveyed European banks have this kind of procedures in place, though figures were expected to increase following the national transpositions of the AML Directive. It is noted that there were significant variations depending on the country. This survey also shows that at the account-opening phase, 75% of the surveyed European banks considered the existence of PEPs as a risk factor triggering the performance of enhanced customer due diligence. See KPMG (2007), p.29 and seq, and p.53. In another survey, limited to the UK, about a third of the participants indicated that one of the biggest challenges faced by their organizations in the future was the requirements linked to PEPs. See PWC (2007b), p.11.

201 According to the KPMG survey of 2007, 61% of the surveyed European banks used commercial lists and a further 29% use a combination of commercial lists with in-house additions. Only 10% of these banks would create their own internal lists.

202 Banks are under significant regulatory and supervisory pressure in this area. The question of the application of the US OFAC lists is regularly raised by banks. See for instance, KPMG(2007), p.54.

203 This appears to be also confirmed by the 2007 KPMG survey, which shows that a significant proportion of banks could not carry out customer monitoring, allegedly because of privacy laws in some countries prevent the sharing of information around the group. See KPMG (2007), p.37. See also in this regard footnote 271.

validated by the parent bank, which is in line with supervisory expectations[204]. Indeed, most banks have developed systems and controls to monitor transactions and detect unusual or suspicious items.

Different methods are used by banks for customer monitoring, such as vigilant staff, sample review of transactions by compliance department; investigation of 'exception by value' reports or the increased used of sophisticated IT monitoring systems[205]. There are advantages in operating this kind of IT systems such as the potential to screen high volumes of transactions and spot patterns of behaviour that may be spread over time or spread over multiple transactions[206]. At the same time, these IT systems appear to be relatively costly (see Annex 6 on cost of compliance) and the human resources implications must not be underestimated (for instance the analysis of potentially suspicious transactions, the need to review false positives etc). Also, it is reported that it is not always easy to calibrate the escalation thresholds in the systems, which contain complex mathematical algorithms.[207] The challenge for banks is to adopt these systems to the right money laundering trends and typologies, for which intelligence sharing with the public sector is key. Customer monitoring with a view to identify terrorist financing patterns is reported to be difficult, notably because of the frequently small value of the associated transactions. In this case, the view has been expressed that enhanced transaction monitoring alone was unlikely to prove a solution to these difficulties, which could trigger the need for increased intelligence sharing between the public and the private sector[208].

---

204 The Basel Committee considers that an "essential element for addressing higher risks is the coordinated approach to the monitoring of customer account activity on a groupwide basis." But it also recognises that such monitoring will be done locally. See Basel Committee (2004), §14 and seq.

205 See KPMG (2007), p.33 and seq. It is reported that around two thirds of the surveyed European banks have recourse to more sophisticated IT monitoring systems. The importance of vigilant staff is, however, also underlined in that survey. This is also confirmed by FSA (2008), p.21 and seq.

206 At the same time, there could be additional benefits arising from these systems, such as improved marketing opportunities and customer relationship management, improved reputational risk management and fraud reduction.

207 KPMG (2007), p.38.

208 KPMG (2007), p.53.

Table A5.1 – Customer identification requirements in national law, regulation or guidance

Requirement	AT	BE	BG	CY	CZ	DE	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL ***	PL	PT	RO	SE	SI	SK	UK
First and last name collected	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	**
Residential address collected	x*	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x	x	x	x	x	x	x	x	
Date of birth collected	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	
Place of birth collected	x*	x	x	x	x	x	x	x	x		x			x		x						x		x	x	
Gender collected					x		x		x	x		x	x			x						x	x**		x	
Customer signature recorded	x*	x	x				x	x	x	x	x	x	x		x	x					x	x			x	
Information on purpose and intended nature of business relationship collected	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	
Information on customer's profession collected	x*	x	x	x	x**		x	x	x	x	x		x			x		x			x			x	x	
Information on customer's public function collected	x	x*	x	x	x				x	x			x	x		x		x	x**		x	x		x	x	
Customer's nationality collected	x*		x	x	x	x			x	x		x	x			x				x	x	x	x		x	
National ID number collected	x*		x	x	x		x	x	x	x		x		x	x		x		x		x	x			x	
National tax number collected	x*		x					x												x				x		
Copy of ID card recorded (passport for no nationals)		x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x			x	x	x ***		x	
Copy of facial picture recorded		x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x			x	x			x	
Reference to the documents used for verifying the identity										x									x					x		
Customer risk profile should be created (on a risk sensitive basis)	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x	x	x	x	

* on a risk sensitive basis

** CZ: only if applicable (e.g. if the account is for business purposes); NL (with regard to PEPs); SE (the social security number is collected, for those customers who have a Swedish social security number, as part of customer identification. It automatically contains info on gender).

*** NL (legislation does not specify what data must be collected, but requires that institutions must identify the customer and verify his/her identity on the basis of documents, data or information obtained from a reliable and independent source. However, it is required that the information as mentioned in this table are kept for 5 years); UK (legislation does not specify what data must be collected, but requires that institutions must identify the customer and verify his/her identity on the basis of documents, data or information obtained from a reliable and independent source. The Joint Money Laundering Steering Group guidance describes the types of information that may be gathered in different circumstances. Institutions should keep copies of, or reference to, the evidence of the customer's identity for five years. Copies may be stored electronically); SE (only collected for customers without Swedish social security number).

Source: Anti-Money Laundering Task Force of CEBS, CEIOPS and CESR and information provided by Member States.

It should be noted that some items may not be directly required by law, but will be part of the normal know-your-customer process undertaken by financial institutions on a risk sensitive basis. Also, some identification items may be contained in official documents collected and this explain why they are not required.

B) Simplified and enhanced customer due diligence

Part B of Annex 5 provides a short description of the national requirements on simplified and enhanced customer due diligence pursuant to the AML Directive. As explained above, banking groups will need to take those national requirements into account when applying a group policy.

Concerning simplified CDD measures, table A5.2 (below) presents a summary of Member States' transposition of Article 11 of the AML Directive as well as Article 3 of Directive 2006/70/EC (Commission's implementing measures).

Concerning enhanced CDD measures, the AML Directive requires their application in at least in the following situations: non-face to face customers (Article 13(2)); cross-frontier correspondent banking relationships with respondent banks from third countries (Article 13(3)) and transactions or business relationships with politically exposed persons (Article 13(4)). In addition, Article 13(1) requires banks "*to apply, on a risk-sensitive basis, enhanced customer due diligence measures […] in situations which by their nature can present a higher risk of money laundering*". These requirements are integrated in national legislation.

In addition, some Member States have integrated in their national legislation additional requirements on enhanced CDD measures:

– BG, with regard to: (i) non-resident customers in BG, as well as off-shore companies, the companies of nominal owners of bearer shares, trust companies and similar structures; (ii) customers, operations and transactions that are linked to states which do not apply or do not completely apply international AML standards.

– CY, with regard to: (i) accounts in the name of companies whose shares are in the form of bearer; (ii) clients accounts in the name of third persons; (iii) private banking customers; (iv) customers providing services of electronic gambling/gaming through the Internet; (v) accounts in the name of trusts; (vi) customers from countries which do not adequately apply FATF's recommendations.

– EL, with regard to: (i) non-residents' accounts, (ii) politically exposed persons, (iii) accounts of companies with bearer shares, (iv) accounts of offshore etc. companies, (v) trusts, (vi) accounts of non-profit organisations, (vii) portfolio management accounts of important clients, (viii) non-face to face business relationships/transactions, (ix) cross-border correspondent banking relationships with respondent banks from third countries, (x) countries which do not comply adequately with the FATF recommendations.

– ES, with regard to: (i) private banking, (ii) distance banking, (iii) currency exchange, and (iv) cross-border transfer of funds.

– FI, with regard to customers or transactions connected with a State whose system of preventing money laundering and terrorist financing does not meet the international obligations.

– FR, with regard to: (i) products or transactions that may favour anonymity; (ii) operations with or clients located in non-cooperative jurisdictions; (iii) cheque cashing or discounting service with foreign institutions; (iv) money transmission services; (v) opening of savings accounts; (vi) paying of life insurance.

– HU, with regard to currency exchange above a predetermined threshold.

– LV, with regard to some high risk situations identified in national regulations. These high risk situations depend on: country risk (e.g. list of non-cooperative countries of the FATF), customer risk (e.g. legal persons issuing bearer shares), risk associated with the economic activity of the customer (e.g. traders in arms and ammunition) or risk associated with the products or services used by the customer (e.g. private banking)[209].

– RO, with regard to: (i) jurisdictions that do not adequately apply AML/CFT requirements; (ii) credit institutions which offer personalized banking services (private banking); (iii) accounts which are not nominated (the identity of the client is known only by the credit institution and it is replaced by a sequential number).

In other Member States (AT, BE, CZ, DE, DK, EE, IE, IT, LT, LU, MT, NL, PL, PT, SE, SI, SK, UK) there are no additional requirements in their national legislation concerning enhanced CDD.

[209] For more detail, see Regulation No 125 of 27 August 2008, available at the website of the Financial and Capital Market Commission of Latvia: www.fktk.lv/en/law/general/fcmc_regulations

Table A5.2 – Simplified CDD requirements

Requirement	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IT	LT	LU	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Art. 11(1): the customer is a credit or financial institution	x	x	x	x	x	x	x	x	x	x	x	x **	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Art. 11(2)(a): listed companies	x	x		x	x	x	x	x	x	**	x		x	**		x	x	x	x	x	x	x	x	x	x	x	x
Art. 11(2)(b): beneficial owners of pooled accounts held by legal profess.	x*	x	x	x	x	x	x	x			x			**		x	x	x	x	x		x	x	x	x	x	x
Art. 11(2)(c): domestic public authorities	x	x	x	x	x	x	x	x	x	**	x		x	**	x	x	x	x	x	x	x	x	x	x	x	x	x
Art. 11(5)(a): life insurance	x	x	x	x	x	x	x	x	x	x	x		x	**	x	x	x	x	x	x	x	x	x	x	x	x	x
Art. 11(5)(b): pension schemes	x	x		x	x	x	x	x	x	x	x		x	**	x	x	x	x	x	x	x	x	x	x	x	x	x
Art. 11(5)(c): employee schemes		x		x	x	s	x	x	x	**	x		x	**	x		x	x	x	x		x		x	x	x	x
Art. 11(5)(d): e-money	x	x		x	x	x	x		x	**	x			**	x	x	x	x	x	x	x	x	x	x	x	x	x
Directive 2006/70/EC, Art. 3(1): EC/EU institutions	x		x	x	x	x	x	x	x				x	**	x	x	x	x	x	x		x	x	x	x	x	x
Directive 2006/70/EC, Art. 3(2): Other financial institutions																		x	x						x	x	
Directive 2006/70/EC, Art. 3(3): low risk products					x	x*		x*						**				x	x	x*			x*	x			x*

* AT (special fiduciary accounts of authorised real estate administrators acting on behalf of joint ownership associations for real state properties); DE (state subsidized, fully funded private pension; capital-forming investment, where the contract meets the conditions for state subsidies; a loan contract, financial leasing contract or instalment sale transaction with a consumer; a loan contract as part of a state subsidy programme carried out by a federal or state development bank, where the loan amount must be used for a designated purpose; credit contract for instalment financing; any other loan contract where the loan account serves the exclusive purpose of repaying the loan and the loan payments are withdrawn from the creditor's account with a credit institution; a savings agreement; a leasing agreement; etc.), EE (transactions with units of an investment fund, with to units of a mandatory pension fund, and with bank accounts held by the pension or social benefit fo natural persons, under certain conditions), UK (children trust fund, other low risk products meeting specified conditions)

** ES (planned in draft law), FR (legislation to be developed with regard to the other situations), IE (planned in draft law)

Source: information provided by national authorities

C) The treatment of the money laundering suspicion

While the policies for risk assessment and detection of suspicious transactions are generally defined at group level (see above), those policies are applied directly at local level. As a result, the analysis of detected transactions that give rise to suspicions and, where applicable, the filing of reports with the FIUs appears to be largely dealt with at local level. Indeed, national legislation does not contain, in general, particular provisions requiring that such analysis is conducted at group level[210]. It appears, however, that it is not necessarily prevented either and it would depend on the possibility to exchange information between parent and subsidiaries/branches on suspicions[211] (see Part D of this Annex).

The filing of "suspicious transaction reports/suspicious activity reports" with the FIUs, follows local laws and procedures. National legislation in EU countries does not require the parent bank to report to the FIU (or to the supervisor) of its own Member State about reports filed by their branches or subsidiaries in other Member States[212]. This is normally not done on a voluntary basis either, unless in exceptional cases when there is a serious reputational risk for the group.

D) Cross border information flows within the banking group

Supervisors attach particular importance to the question of cross-border intra-group sharing of information, in particular on higher risk customers and activities relevant to the global management of reputational and legal risks[213]. This question is possibly the most difficult one for banks when implementing an AML compliance policy at group level. The main reason for this is the balance between the AML requirements, on the one side, and the personal data protection legislation and/or banking secrecy regulations, on the other side. Different scenarios may be envisaged on intra-group information flows, depending if they concern: (i) customers; (ii) suspicions; (iii) reports filed with the FIUs (and related issues); or (iv) feedback from FIUs. Additionally (v) these flows may be linked to the question of record keeping.

(i) Information flows on customers (not linked to a suspicion)

---

210 In BG, reporting entities are obliged by the law to apply a group policy with regard to the management of the money laundering suspicion.

211 In some countries, some legislative provisions seem to be indirectly related to this issue. For instance, according to the IT law, financial intermediaries belonging to the same group may use a single service centre to keep and manage their own archives to that a delegate may extract integrated records at group level, including for the purposes of reporting suspicious transactions to the FIU. In SE there is no explicit requirement in the new law of a group policy as such, but the FSA's secondary regulation (which is directly enforceable) FFFS 2009:1 requires that a central function within a group is designated with the responsibility to make sure that the legally stipulated reporting requirements (which mirror those of the 3rd AML directive) are met by a group. In addition to this the secondary regulation also contains specific provisions on internal control mechanisms within a group in order to make sure that the requirements in the new law *are* actually met.

212 A paradoxical case may arise when the bank has no branch or subsidiary in a State where it provides financial services. In such a situation, it would report to the FIU of its own Member State about suspicious transactions.

213 See Basel Committee (2004), §§17-19. In particular the Basel Committee recommends that the "*bank's centralised KYC function should evaluate the potential risk posed by activity reported by its branches and subsidiaries and where appropriate assess its world-wide exposure to a given customer*." *Ibid*. §18.

In almost all of Member States[214], the national AML legislation does not explicitly restrict the circulation of information regarding customers within the banking group for the purposes of applying customer due diligence measures. Additionally, in one Member State[215] there is a possibility to use a single service centre to keep and manage customers archives consolidated at group level which may be used by the AML officers of the different entities of the group.

In practice, the perception of the banking associations is that, in the majority of cases, flow of information within the group with regard to customers would not take place due to the restrictive effects resulting from national legislation on data protection (or the application thereof) and general rules on banking secrecy (where they exist). Anecdotal evidence suggest that banking groups tend to overcome these difficulties through on-site visits by head office/parent bank staff, who then are able to report back to headquarters.

This situation does not seem to match the supervisory recommendations. The Basel Committee warns about legal impediments to the transfer of customer information to head offices, which may conflict with the consolidated KYC objective[216]. It should be note in this regard, however, that it is unclear whether the Basel Committee has taken into account the fundamental right dimension of the legislation on the protection of personal data.

(ii) Information flows on suspicions, prior to the formalisation of a report

An adequate treatment of suspicions within a banking group, aiming at determining whether the filing of a suspicious transaction report is necessary, may require an information exchange with other entities within the group on the suspicious case (as well as on previous suspicious transaction reports established on the same customer within the group. In several Member States there are no restrictions in the national AML legislation concerning the transmission of information within the banking group on suspicious transactions prior to the formalisation of a report to the FIU (or the decision not to make one), and at least in one of them[217] it is required by law to provide the other entities of the group with information necessary to combat money laundering (or terrorist financing). For some of these Member States, Article 28(1) would not prevent such transmission as it would only prohibit disclosure of the fact that a report was filed (or will be) with the FIU[218]. For others, irrespective of the interpretation of Article 28(1), Article 28(3) of the Directive would be interpreted as allowing for such transmission of

---

214 AT, BE, BG, CY, CZ, DE, DK, EE, EL, ES, FI, FR, HU, IE, IT, LT, LU, LV, MT, NL, PT, RO, SE, SI, SK and UK.

215 IT

216 The Basel Committee considers "*essential that all jurisdictions that host foreign banks provide an appropriate legal framework which allows information for KYC risk management purposes to be passed to the head office/parent bank.*" The Basel Committee also believes that "*there is no justifiable reason why local legislation should impede the passage of customer information from a bank branch or subsidiary to its head office or parent bank for risk management purposes*". It further states that "*if the law restricts disclosure of information to "third parties" it is essential that the head office or parent bank is clearly excluded from the definition of a third party*." Finally, the Basel Committee urges jurisdictions that have legislation that impedes, or can be interpreted as impeding, such information sharing, to remove any such restrictions and to provide specific gateways. See Basel Committee (2004), §§24-27, in particular §27.

217 FR.

218 BE, SI. For other Member States, such as DE, the prohibition in Article 28(1) would capture data related to the preparation of a report to the FIU. Also, the question of the interpretation of "third person" in Article 28 would appear with regard to branches. To the extent that the branch and the parent institution are the same institution, one could interpret Article 28(1) as not prohibiting the cross-border flow of information within the same institution.

information (i.e. the formation of the suspicion being an operation which serves the purpose of compliance with the obligation to file a "suspicious transaction report")[219].

Some countries have provided for explicit safeguards in this regard, such as: the information disclosed in this manner should only be exchanged between the AML compliance departments responsible for making the reports, to the exclusion of other staff members[220]; or such disclosures should not undermine an investigation by the authorities[221].

Nevertheless, in other Member States, it is not possible[222] to share information within the group on suspicious transactions prior to the formalisation of a report with the FIU (only after the report is filed with the FIU such transmission would be possible), or it is not foreseen[223]. In one Member State[224], an intermediate situation is foreseen. On the one hand, the legislation only provides for the transmission of information within the group if a report has been made. On the other hand, it is possible to use the single service centre on customer information referred to above (Part D (i) of this Annex) also for the purposes of reporting suspicious transactions.

In practice, according to the banking associations, information on suspicious cases is rarely shared within the group. This would happen only in exceptional cases, covered by agreements/protocols under the control of the parent bank that guarantee confidentiality and secure transmission of data. The banking associations' perception in this regard is that national data protection laws and bank secrecy rules would generally prevent the circulation of this kind of data between institutions of the same group (see above Section 6.3).

(iii) Information flows on reports filed with the FIUs

The possibility of circulating, within the banking group, information on reports filed with the FIUs is provided for in Article 28(3) of the AML Directive. Almost all Member States have integrated this provision in national law. One Member State[225], however, decided not to allow for the intra-group disclosures relating to reports filed with the FIU. Similar safeguards[226] as above would also apply here.

It should be noted in this regard that FIUs within the EU are not particularly supportive of the intra-group sharing of information on reports filed with them. While recognising that the derogation in Article 28(3) of the AML Directive satisfies "*the need to reinforce the fight against money laundering and facilitate within groups the integration of the risk-based approach logic*", this sharing of information raises, from the FIUs' point of view, a number of matters of principle "*as regards professional secrecy and confidentiality, the principle of territoriality, the cooperation between FIUs, data protection, [and] the secure feedback of*

---

219 AT, CY, CZ, DE, DK, EE, EL, FR, HU, MT. Such transmission of information is also accepted in BG, EE, FI, HU, LT, LU, RO, SE and UK, but it is not explicit if on the basis of the interpretation of Article 28(3).

220 FR.

221 UK.

222 PL, SK. In NL, the law requires that the report with the FIU is done immediately. Therefore, de facto it is not possible to share information within the group before formalising the report.

223 PT.

224 IT.

225 SI, with regard to disclosures between parent bank and subsidiary. However, information flows between branch and head office are possible.

226 Cf. Part D (ii) of this Annex, regarding the staff able to access the exchange of information.

information to disclosing professions".[227] They also underline that there is a risk of abusing the permission for this kind of intra-group exchanges of information and circumvent other prohibitions of disclosure.[228]

(iv) Information flows on feedback from FIUs

In principle, no restrictions exist for the circulation of information within the banking group about trends, typologies or general feedback received from FIUs or other public authorities, provided it does not include precise information on clients or their transactions related to on-going procedures. Concerning feedback on on-going particular cases including data on clients and transactions – when provided,[229] legislation in a few countries allows for the intra-group circulation of such feedback[230]. Nevertheless, national legislation is in most cases silent[231] and thus open to interpretation. In some countries, legislation could be interpreted that the circulation of specific feedback within the group is permissible (i.e. in the absence of prohibition) for AML purposes[232]. The practice is also that such circulation would be possible with the express authorisation of the FIU[233] – otherwise, the information should remain the AML compliance department of the reporting entity[234]; or FIUs would discourage dissemination by clearly marking such feedback as confidential[235]. In any event, general rules on data protection and bank secrecy would apply: for instance in two countries[236], the "need-to-know" principle would apply to such information flows. Finally, in one Member State[237], legislation explicitly foresees that FIU feedback with regard to specific reports cannot be disclosed within the institutions belonging to the same group, only the report itself can be.

(v) The question of record keeping

According to the banking associations, due to regulatory requirements, information is archived in each local jurisdiction, without connection between databases. For instance, in one

---

227 See EU FIU Platform (2008), p.14-15. FIUs particularly underline the risk that information is circulated in an unsafe manner. They also warn about the possible creation of parallel channels of information exchange outside the framework of official secured mutual cooperation between FIUs given that an FIU might obtain information from the national branch or subsidiary of a group that has obtained such information within the framework of intra-group exchanges. They also indicate that there is a risk of duplicating the FIU's work in this regard. The principle of territoriality related to the transmission of suspicious transaction reports could accordingly encounter difficulties with respect to its application due to possible centralisation of reports of suspicious transactions within the parent companies of groups.

228 For instance, in order to circumvent the prohibition to provide information following a request by the judicial authorities, banks could disclose the same information to the FIU and then pretend to be entitled to circulate the information within the group. See EU FIU Platform (2008), p.16.

229 This type of specific feedback is not always provided by FIUs. In some cases, feedback is limited to either general feedback or to publicly available information (e.g. outcome of the judicial procedures). On feedback, see generally B & S Europe (2009).

230 DK, HU, LU, LV, SK. At least in one case, Article 28(3) of the AML Directive has been interpreted as allowing intra-group circulation of information regarding specific feedback on previously filed suspicious transaction reports.

231 AT, BE, BG, CY, CZ, DE, EE, EL, ES, FR, IE, IT, LT, MT, PL, PT, RO, SE, SI.

232 AT, DE, EE, IE, IT, LT, PT, RO, SE, SI

233 FIUs are, in general, not too favourable to the disclosure of feedback within the banking group. See EU FIU Platform (2008), p.13-14.

234 BG, CY, FI, RO, UK.

235 IE, MT.

236 DK, MT.

237 NL.

Member State the data retention period is longer than the one foreseen in the Directive[238]. As a result, centralised archiving at group level of the information collected by different Member States is not really feasible, although it could be an efficient way of ensuring that records are easily retrievable and logged. This also implies that it is not possible for an institution to organise a centralised system covering operations in different Member States in order to comply with the requirements of Article 32 of the Directive.[239]

238 In ES and SI, the data retention period is 6 years.

239 There are efficiency arguments in favour of such a centralised system: for instance, a centralised system would ensure a consistent approach and the smooth the transfer of knowledge around requests for information from local FIUs. At the same time, the key factor is that the information can be retrieved quickly, rather than the actual location of the records.

ANNEX 6 – THE COST OF COMPLIANCE

The cost of compliance with AML requirements is not insignificant and has increased in recent years following the regulatory changes introduced in the EU, notably the AML Directive[240].

A recent external study has examined for the Commission the cost impact of compliance for certain types of firms within the financial industry (including banks) with six key EU directives in the financial services area, including the AML Directive[241]. The study focuses on the so-called 'incremental compliance costs' caused by regulation, not on the total costs of activities that happens to contribute to regulatory compliance[242].

The study identifies separately cost impacts that are of one-off nature (i.e. those costs that only have to be incurred once in making the transition, such as IT investment and the re-shaping of business processes) from those that are recurring in nature (on-going costs as a result of regulation). The ongoing costs of compliance for any given firm are typically lower than the one-off costs. Looking at the different sectors surveyed, recurring costs are mostly between 15 and 20 per cent of the implementation cost recorded (with some exceptions)[243]. Figure 6.1 illustrates this divergence in scale, by showing the dispersion of the results obtained for the AML Directive.

This study shows that firms have adopted different strategies in approaching the implementation of the Directive both regarding one-off (in particular, in their willingness to put maximum reliance upon the automation of processes) and ongoing costs. The dispersion in the ongoing costs — and general business experience — suggest that firms have experienced differing levels of success in achieving this objective. Indeed the study shows a wide dispersion of results.

---

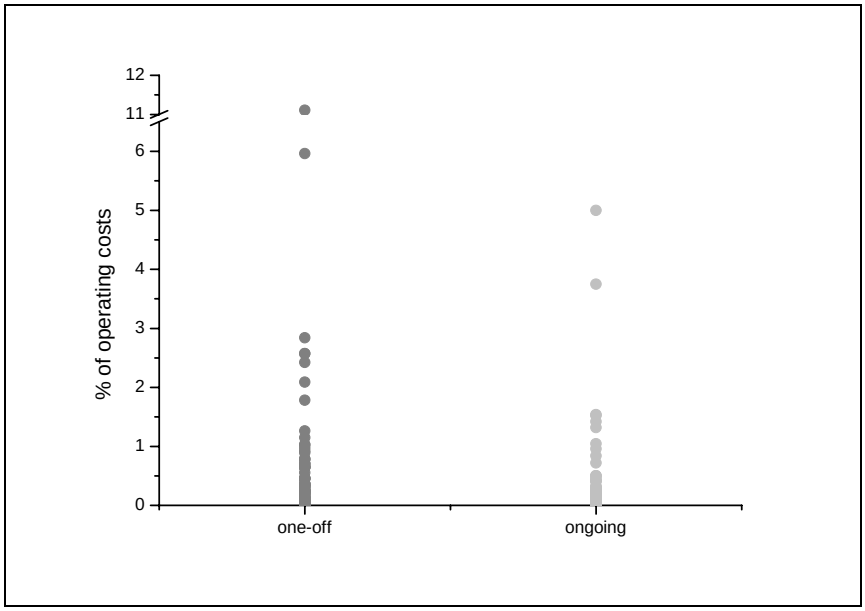
240 See CRA International (2009), p.13. According to the KPMG survey of 2007, a range of European banks estimated that their AML compliance costs increased by 58% over the 2004-2007 period. This survey also predicts that costs will grow at a slower rate in the following years: indeed European banks expect these costs to increase by 27% between 2007 and 2010. This survey underlines the difficulty of estimating AML costs as they may be spread across many different functions (operations, compliance, risk) or regions, involve direct and indirect costs, and overlap with processes that are embedded in normal business practice (e.g. credit risk or customer relationship management). This survey does not make a distinction between one-off and on-going costs of compliance. See KPMG (2007), p.14 and seq.

241 Europe Economics (2009). The survey concentrated on firms from four sectors within the financial services industry in the EU: banks and financial conglomerates, asset managers, investment banks and financial markets. The six directives concerned are the so-called Prospectus Directive, the Financial Conglomerates Directive, the Capital Requirements Directive, the Transparency Directive, the Markets in Financial Instruments Directive – MiFID and the AML Directive. These measures were part of the Commission's Financial Services Action Plan (FSAP) of 1999 (the so-called 3rd AML Directive of 2005 replaced in the meantime the precedent, second, AML Directive of 2001 which was the measure addressed in the FSAP).

242 *Ibid*., §2.14. For an explanation of the methodology of this study, see: section 2; the introductions to sections 4 and 5; as well as Appendix 1 of the final report.

243 *Ibid*., §15 and seq..

Figure 6.1: Dispersion of one-off and ongoing costs of the AML Directive (expressed as a percentage of 2007 operating expenses)



Source: Europe Economics (2009), figure 3.

A) The one-off costs of compliance

Concerning the one-off costs of compliance (see Table 6.1) for banks, financial conglomerates and investment banks, compliance with the AML Directive roughly accounts for 10% of all their financial services regulatory costs.

TABLE 6.1 – AML Directive – One-off costs of compliance

	Banks & financial conglomerates	Investment banks	Asset managers	Financial markets
Mean[244] (percentage of 2007 operating expenses)	0.29%	0.23%	0.21%	0.16%
Median[245] (percentage of 2007 operating expenses)	0.31%	0.32%	0.24%	0.03%
Total financial services regulatory compliance costs[246] (percentage of 2007 operating expenses)	2.90%	2.25%	1.58%	3.40%
Mean: average absolute value of the incremental cost changes, per firm (€000s)	4,588	2,507	825	33
Total financial services regulatory compliance costs (€000s)	45,149	24,569	5,565	694
Average of operating costs (€000s)	1,558,072	1,030,071	384,582	20,403

Source: Europe Economics (2009), tables 4.1, 4.2 and 4.3.

The difference in cost between banks and financial conglomerates on the one side, and investment banks, on the other side, possibly owes to a typically different client make-up[247].

244 The middle value in a series of data points arranged sequentially. The sequence from which this median has been selected is based upon the estimated one-off costs of compliance expressed as a percentage of the relevant firm's more recent operating expenditure.

245 Aggregate one-off costs of compliance expressed as a percentage of the relevant firms' aggregated most recent operating expenditure. This implies that the experience of the larger firms will carry more weight in the sample presented.

246 Including other FSAP measures and other financial services regulation, whether EU, nationally or extra-territorially derived.

The study also notes that in the AML field, firms voluntarily practice standards that are applied globally, which adds on to the costs of the AML Directive[248]. If a comparison is done with the costs of compliance for asset managers, Table 6.1 shows that the one-off costs of compliance with the AML Directive take a higher proportion of asset managers' total costs[249].

Out of the six directives examined by the study, the AML Directive comes third in terms of cost impact for banks, financial conglomerates and investment banks, behind the Capital Requirements Directive and MiFID. These two other directives represented the most important regulatory changes in this area in recent times and their compliance costs are significantly higher[250]. It is interesting to note in this regard that the study identifies the possibility for firms to achieve synergies between some of the requirements in the AML Directive and MiFID: a small number of institutions surveyed did feel that synergies had been achieved (or could be achieved) between the "know-your-customer" requirements of the AML Directive and suitability tests of MiFID[251]. Nevertheless, very few businesses believed that any significant cost-reducing synergies had been achieved in the implementation of the various measures: the variation in the implementation dates was the most frequently cited factor behind this. Another component to this problem was that firms felt that the detail necessary to properly prepare for IT changes was not always forthcoming from the implementing authorities in a sufficiently timely manner.

The main source of AML Directive related compliance spending is on IT (see Table 6.2 for banks and financial conglomerates and Table 6.3 for investment banks).[252] Similarly high IT costs appear for almost all the directives covered.

TABLE 6.2 – Cost drivers of the selected directives (banks and financial conglomerates) – one-off costs

Directive	Prospectus	FCD	CRD	Transparency	MiFID	3AMLD
Familiarisation with Directive	49%	15%	2%	13%	3%	3%
Consultancy fees	5%	11%	20%	5%	13%	11%
Legal advice	23%	5%	5%	5%	7%	1%
Training	13%	8%	5%	11%	15%	22%
Staff recruitment costs	0%	2%	4%	1%	2%	2%
Investment in/updating IT	2%	47%	57%	63%	52%	54%
Project management	8%	9%	8%	3%	7%	7%
Other	0%	2%	0%	0%	0%	0%

Source: Europe Economics (2009), table 4.10.

247 *Ibid*., §4.10. The study also provides further breakdowns of costs, per size and geographical origin. See §4.20 to 4.25 and 4.93 to 4.94.

248 *Ibid*., §4.12 in fine. The non-EU regulation costs are reflected in the study, on an aggregated basis, in the total costs.

249 Financial markets (e.g. stock exchanges operators) are not directly subject to the obligations of the AML Directive. But in order to allow for comparisons, their costs are also shown in Table 6.1.

250 *Ibid*., tables 4.1, 4.2 and 4.3. The impact of MiFID costs doubles those of the AML Directive, while CRD accounts for more than half of the total financial services regulatory compliance.

251 *Ibid*., §§4.14 to 4.17. This is also confirmed by the KPMG survey of 2007. See KPMG (2007), p.53.

252 See generally, *Ibid*., §§4.57 to 4.62, and §§4.106 to 4.107.

TABLE 6.3 – Cost drivers of the selected directives (investment banks) – one-off costs

Directive	Prospectus	FCD	CRD	Transparency	MiFID	3AMLD
Familiarisation with Directive	9%	7%	3%	7%	6%	5%
Consultancy fees	13%	0%	19%	10%	16%	12%
Legal advice	18%	10%	2%	4%	4%	6%
Training	14%	15%	2%	4%	10%	13%
Staff recruitment costs	4%	0%	1%	10%	1%	0%
Investment/ updating IT	27%	39%	62%	36%	49%	53%
Project management	14%	29%	10%	29%	14%	12%
Other	0%	0%	1%	0%	1%	0%

Source: Europe Economics (2009), table 4.27.

In terms of IT spending[253], this included projects designed to: (i) meet the "Know-Your-Customer" informational requirements, such as some adaptation of the existing Customer Relationship Management systems and/or some new data entry needed to meet these increased data capture requirements (in a few instances, this triggered data warehousing projects to enhance inter-system data capture); (ii) facilitate increased monitoring of suspicious transactions through increased automation of processes[254]; (iii) facilitate Politically Exposed Persons screening; and (iv) assist in risk assessment.

Training and (for larger banks) external consultants are also important sources of cost. According to this study, the importance of training in the AML field is driven by it being more generally applicable than the other Directives: in other words, the breadth of coverage of the training believed to be necessary to comply with this measure was greater than for the others. There was also some cost associated with the re-design of training programmes and the roll-out of these[255].

These findings are fundamentally not different from those of a different (and qualitative) survey conducted in 2007. According to that survey, the drivers of higher expenditure in the 2004-2007 period appear to be greater expenditure on transaction monitoring capabilities and upgrades to existing systems, and the provision of additional tailored training to staff (in that survey there was no distinction between one-off and on-going costs).[256]

The study notes that the implementation of the AML Directive remains a work-in-progress. Trans-national businesses have typically implemented its provisions on a group basis, either using the Directive itself as guidance or the implementation in their own Member State (if it had been implemented). Their expectation is, however, that additional expenditure will be necessary in the future to get adapted to the requirements of the local transposition. Some participants argued that the uneven transposition situation discouraged early adoption[257].

253 *Ibid*., §§4.58 and 4.59.

254 A different survey carried out in 2007 by a consultancy firm found that transaction monitoring is the single greatest area of AML expenditure for banks. See KPMG (2007), p.16 and 33.

255 Europe Economics (2009), §§4.57 and 4.60.

256 Respondent banks estimated the areas of greatest AML expenditure according to the following categories (the ranking is based on a maximum score of 5 for 'very strong impact' and a minimum score of 1 for 'no impact'): enhanced transaction monitoring (4.1); greater provision of training (3.4); sanctions compliance (3.4); remediation of KYC documentation for existing customers (3.3); transaction 'look-bank' reviews (3.2); increased external reporting requirements 3.2); introduction of global procedures (3.0); more complex account-opening procedure (3.0); and increased internal reporting requirements (2.8). See KMPG (2007), p.16.

257 Europe Economics (2009), §4.62.

B) The ongoing cost of compliance

Concerning the ongoing cost of compliance (see Table 6.4) for banks, financial conglomerates and investment banks, compliance with the AML Directive roughly accounts for 13% of all their financial services regulatory costs[258]. In relative terms, this is a slightly higher figure than the one-off cost of compliance, possibly explained by the relatively lower on going costs of compliance with the Capital Requirements Directive and MiFID. In any event, as for the one-off costs, these two other directives bear the bulk of the compliance costs, with the AML Directive ranking third out of the six directives examined by the study. If a comparison is done with the ongoing cost of compliance for asset managers, Table 4 shows that the ongoing cost of compliance with the AML Directive take a lower proportion of asset managers' total costs, which is explained by the higher ongoing cost incurred by asset managers regarding MiFID and Prospectus Directive[259].

TABLE 6.4 – AML Directive – Ongoing cost of compliance

	Banks & financial conglomerates	Investment banks	Asset managers	Financial markets
Mean[260] (percentage of 2007 operating expenses)	0.08%	0.05%	0.07%	0.13%
Median[261] (percentage of 2007 operating expenses)	0.09%	0.08%	0.07%	0.00%
Total financial services regulatory compliance costs[262] (percentage of 2007 operating expenses)	0.59%	0.38%	0.85%	1.70%
Mean: average absolute value of the ongoing costs incurred, per firm (€000s)	1,195	464	278	27
Total financial services regulatory compliance costs (€000s)	8,540	3,807	2,532	347
Average of operating costs (€000s)	1,558,072	1,030,071	384,582	20,403

Source: Europe Economics (2009), tables 5.1, 5.2 and 5.3.

The most important ongoing costs of compliance with the AML Directive concern IT expenditure and additional staff costs (see Table 6.5 for banks and financial conglomerates and Table 6.6 for investment banks).[263] Most of the IT expenditure is linked to access costs to various databases dedicated to the tracking and screening of relevant parties such as Politically Exposed Persons, watch lists etc. Whilst some firms (generally larger banks) see automation as the only way to provide the necessary evidence of an audit trail to the regulatory authorities in the event of problems arising (as well as being cost effective by comparison to manual effort), a number of firms have retained significant (or total) human oversight in this area.

---

258 The study also provides further breakdowns of costs, per size and geographical origin. See §§5.12 to 5.17 and 5.62.

259 Financial markets (e.g. stock exchanges operators) are not directly subject to the obligations of the AML Directive. But in order to allow for comparisons, their costs are also shown in Table 6.4.

260 The middle value in a series of data points arranged sequentially. The sequence from which this median has been selected is based upon the estimated ongoing costs of compliance expressed as a percentage of the relevant firm's more recent operating expenditure.

261 Aggregate ongoing costs of compliance expressed as a percentage of the relevant firms' aggregated most recent annual operating expenditure. This implies that the experience of the larger firms will carry more weight in the sample presented.

262 Including other FSAP measures and other financial services regulation, whether EU, nationally or extra-territorially derived.

263 See generally, *Ibid*., §§5.34 to 5.40 and §5.69.

TABLE 6.5 – Cost drivers of the selected directives (banks and financial conglomerates) – ongoing cost

	Prospectus	FCD	CRD	Transparency	MiFID	3AMLD
Additional staff	37%	6%	43%	15%	35%	37%
Internal reporting	2%	7%	8%	4%	7%	4%
IT	15%	6%	26%	49%	28%	31%
External reporting	16%	65%	10%	8%	10%	5%
Training	19%	4%	6%	8%	10%	13%
Audit	10%	11%	7%	15%	9%	10%
Other	0%	0%	0%	0%	0%	0%

Source: Europe Economics (2009), table 5.10.

TABLE 6.6 – Cost drivers of the selected directives (investment banks) – ongoing cost

Directive	Prospectus	FCD	CRD	Transparency	MiFID	3AMLD
Additional staff	0%	0%	34%	33%	26%	23%
Internal reporting	0%	23%	7%	7%	6%	12%
IT	1%	35%	32%	19%	45%	29%
External reporting	48%	12%	10%	8%	13%	9%
Training	47%	31%	6%	12%	6%	16%
Monitoring/audit	3%	0%	10%	21%	4%	10%
Other	0%	0%	0%	0%	0%	0%

Source: Europe Economics (2009), table 5.27.

Ongoing training is not insignificant. However, it is highlighted that once e-learning or class-based training modules are developed (see one-off costs), the ongoing requirement in cash cost terms is mitigated[264]. It is also noted that whereas large banks spent proportionately more than small ones on training as a one-off cost, the proportion of training within ongoing costs is less. This would be consistent with larger banks being more reliant on e-learning and e-training.[265]

264 Interviewees in the study were not in agreement as to whether the AML Directive increased the intensity of training required — i.e. whether or not the duration of the training sessions increased or were rolled out to a broader set of employees. See *Ibid*. §5.36.

265 Some participants remain sceptical about e-learning generally. It is seen by such firms as a "quick fix", in essence allowing maximum access to training for more people in less time. However, these firms considered it inevitable that it would require supplementation by more traditional (and more expensive) classroom-based approaches. See *Ibid*. §§5.37 and 5.38.

ANNEX 7 – DATA PROTECTION RULES AND AML OBLIGATIONS

This annex provides a summary of the issues raised by stakeholders in this survey concerning the relation between data protection rules and AML obligations. This annex does not aim at providing a comprehensive view on this issue.

Concerning the **information on the customer** necessary for the customer acceptable policy, different rules at national level provide in some cases for different documentation evidence (see Part A of Annex 5). Additionally, the risk-based approach in the AML Directive gives institutions a large margin of manoeuvre as regards the information to be collected. This raises questions among stakeholders as to whether there are limits to the type of information that can be circulated within the group or stored at group level. In the same manner as banks need to demonstrate to the banking supervisors that the extent of the customer due diligence measures is appropriate in view of the risk of money laundering, banks would also need to justify to the data protection authorities that the processing in question, involving intra-group and cross-border transfer of information, complies with data protection rules, namely the legitimacy of the processing and the necessity, proportionality and purpose limitation of the processing (i.e. that the collection and further processing of personal data is lawful, necessary, adequate, relevant and not excessive in relation to the purposes for which the data was collected)[266].

Regarding the legitimacy of the processing, from the point of view of data protection law, the intra-group transfer of persona data within the EU is acceptable if it is grounded on any of the specific legal basis provided for in Directive 95/46/EC; for instance it could be argued that the processing is necessary for the purposes of the legitimate interests pursued by the data controller (e.g. the subsidiary) or by the third party (e.g. the parent bank) to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject[267]. The question raised by stakeholders is whether the prevention of money laundering can systematically be considered as being a legitimate interest of both institutions implied in the exchange of information. This would be a kind of subjective test, based on the needs of the bank. On the contrary, any need to justify these legitimate interests on a case-by-case basis, depending on the individual circumstances of each particular case, could render any systematic circulation of data within the group or record keeping of data at group level impractical. The question of the prevailing interests for fundamental rights and freedom of the data subject would also need further examination in this regard[268].

In order to overcome this difficulty, some banks have recourse to standard consent clauses, included in the banks' general terms and conditions, which provide for the possibility to make intra-group transfer of information. However, this leaves the possibility to undertake this processing in the hands of the data subject (who could object to it) or might be subject to legal

---

266 See Article 6(c) of Directive 95/46/EC.

267 See Article 7(f) of Directive 95/46/EC. It is arguable whether the intra-group processing could be considered necessary for compliance with a legal obligation to which the bank is subject (cf. Article 7(c) of Directive 95/46/EC).

268 For instance, it could be conceivable that the data subject refuses his/her consent to the processing of certain types of personal data on the ground that such processing is not necessary for the purposes of complying with the AML obligations. This could be particularly the case in connection to the monitoring of the business relation, where the directive rules are vague.

challenge on the grounds that the data subject has not unambiguously given his specific, free and informed consent)[269]. The requirement of respecting the fundamental rights and freedoms of the data subject that could impede intra-group data flows would also deserve attention.

The question of the further processing of data[270] has been raised, in connection to the **customer and transaction monitoring**: e.g. are there limits to the central storage of client information at group level for the purposes of transaction monitoring by different entities within the group in an EU cross-border context? Also, are there limits to the possibility of generating (and storing) a global profile of the customer (i.e. across different jurisdictions which can be shared intra-group)? In this context, one would need to clarify whether the systematic sharing of customer information within the group is compatible with the specific, explicit and legitimate purposes initially identified for the collection of data, or whether a case-by-case justification would be needed. In the latter case, the customer and transaction monitoring at group level might not be practical.

The use of **sanction lists** poses particular challenges and leads to legal risks. Banking groups would tend to use, at group level, a consolidated list of all national lists applicable to the group. However, there may be impediments at national level resulting from national data protection safeguards: e.g. this processing may result in blacklisting or could be considered to involve the processing of sensitive data such as ethnic origin or religion[271].

Concerning the intra-group transfer of information on **suspicious transactions** and on reports thereof, a question arises as to whether the absence of prohibition in the national legislation transposing the AML Directive is a sufficient legal basis for the transfer of data within the banking group from the point of view of data protection rules and whether such intra-group transfer of information meets data protection principles of necessity, proportionality and purpose limitation. For some Member States AML authorities this would not be clear enough. For others, the presumption is that there should not be a problem from the perspective of respecting the fundamental right to the protection of personal data. An additional issue raised in connection to the processing of suspicious transactions is that the intra-group circulation of information or the record keeping at group level should not amount to blacklisting[272].

---

269 The Basel Committee survey on the implementation of its compliance principles identifies the customer consent requirement as a restriction to the information sharing within groups for compliance purposes. See Basel Committee (2008), §11 and §§54-61.

270 "*Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.*" Cf. Article 6(b) of Directive 95/46/EC

271 Particular attention should be given in this context to the recent case law of the Court of Justice on the lawfulness of restrictive measures taken against individuals by EC Regulations adopted to implement sanctions adopted by the UN Security Council. The Court of Justice has stressed the need that such legal measures respect fundamental rights, namely the fundamental right to judicial protection and the right to be heard. (Decision of 3.9.2008, cases C-402/05 P and C-415/05 P (Kadi) OJ C 285 of 8.11.2008; p. 2).

272 In SI, the attempt by a subsidiary of an EU bank to create a database with suspicious information connected to money laundering (not necessarily transmitted to the local FIU) and transmit this information to the head office was unsuccessful, as a result of the strict domestic legislation not accepting the creation of black lists.

REFERENCES

B & S Europe (2009), *Study on Best practices in vertical relations between the Financial intelligence Unit and (1) law enforcement services and (2) Money Laundering and Terrorist Financing Reporting entities with a view to indicating effective models for feedback on follow-up and effectiveness of suspicious transaction reports*, Study conducted for the European Commission. Forthcoming.

Basel Committee (2004): Basel Committee on Banking Supervision, *Consolidated KYC Risk Management*, October 2004

Basel Committee (2005): Basel Committee on Banking Supervision, *Compliance and the compliance function in banks*, April 2005.

Basel Committee (2006): Basel Committee on Banking Supervision, *Enhancing corporate governance for banking organisations*, February 2006.

Basel Committee (2008): Basel Committee on Banking Supervision, *Implementation of the compliance principles – A survey*, August 2008.

CEBS (2009): Committee of European Banking Supervisors, *Mapping of supervisory objectives and powers, including early intervention measures and sanctioning powers*, CEBS 2009 47, March 2009.

CRA International (2009): *Evaluation of the economic impacts of the Financial Services Action Plan*. Study conducted for the European Commission. Forthcoming.

De Larosière Group (2009): High-Level Group on Financial Supervision in the EU – chaired by Jacques de Larosière, *Report*, February 2009.

EU FIU Platform (2008): EU Financial Intelligence Units' Platform, *Report on confidentiality and data protection in the activities of FIUs (good practices)*, 28 April 2008.

European Commission (2009), *Communication of 4 March 2009 for the Spring European Council – Driving European recovery*, COM(2009)114.

Europe Economics (2009), *Study on the cost of compliance with selected FSAP measures*, Study conducted for the European Commission.

FATF (2007): Financial Action Task Force, *Guidance on the risk-based approach to combating money laundering and terrorist financing*, June 2007.

FSA (2008): Financial Services Authority (United Kingdom), *Review of firms' implementation of a risk-based approach to anti-money laundering (AML)*, March 2008.

Group of Twenty (2008), *Declaration of regarding the Summit on Financial Markets and the World Economy*, 15 November 2008.

Group of Twenty (2009a), *Leaders' Statement (London Summit)*, 2 April 2009.

Group of Twenty (2009b), *Declaration on strengthening the financial system (London Summit)*, 2 April 2009.

The Joint Forum (2005), *Initiatives taken by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism*, January 2005.

JMLSG (2007): Joint Money Laundering Steering Group, *2007 Guidance.*

KPMG (2007), *Global Anti-Money Laundering Survey 2007 – How banks are facing up to the challenge.*

PWC (2007a): PriceWaterhouseCoopers, *Economic Crime: people, culture and controls (the 4th Biennial Global Economic Crime Survey).*

PWC (2007b): PriceWaterhouseCoopers, *Anti-Money laundering survey*.