On the frontline against money-laundering: the regulatory minefield

Liliya Gelemerova

Crime Law Soc Change (2009) 52:33–55
DOI 10.1007/s10611-008-9175-8

On the frontline against money-laundering: the regulatory minefield

Liliya Gelemerova

Published online: 3 December 2008

Abstract Intelligence gathering plays a vital role in the 'war' against money laundering. Particularly important in this intelligence gathering process is the global network of Financial Intelligence Units (FIUs) fed by a host of auxiliary (primarily financial) institutions required to report suspicious transactions. This paper briefly reviews the history of the international system of anti-money laundering measures imposed on the financial industry and other regulated businesses, the development of the global network of FIUs and their system of information gathering. It will examine some of the issues that arise from the regulatory framework within which this information gathering takes place. It will also address the issue of instrumental clarity and whether existing and new directives, requirements and approaches are sufficiently clear to enable reporting institutions on the 'front-line' to operate effectively.

Introduction

Intelligence gathering has played a paramount role in every war. The 'war' against money laundering has been no exception. It started about twenty years ago as an extension of the battleground for the war on drugs; and in the aftermath of 11 September 2001 it became fused with the new war on terrorism of which the fight against the financing of terrorism has become an integral part. With the increasing importance of intelligence in this war, the scope for financial intelligence gathering has grown commensurately. Legislative developments in this field have, therefore, risen to unprecedented levels of information collection, allocation and dissemination. Particularly critical in the arsenal of governments internationally has been the global network of Financial Intelligence Units (FIUs)[1] fed by a host of auxiliary (primarily financial) institutions required to report suspicious transactions. How has the

[1] FIU is defined on pp. 5-6 of this article.

Liliya Gelemerova is a doctoral (PhD) student at Tilburg University and Senior Investigator at Nardello & Co.

L. Gelemerova (✉)
Nardello & Co. LLP, 13 Harley Street, London W1G 9QG, UK
e-mail: lgelemerova@nardelloandco.com

financial intelligence concept unfolded and been cast into regulations, and how have the facilitators of intelligence (the reporting institutions, i.e. financial and other institutions that are required to report suspicious transactions to the respective FIUs) responded to the new challenges brought about by these trends?

This paper briefly reviews the history of the international system of anti-money laundering measures imposed on the financial industry and other regulated businesses, the development of the global network of FIUs and their system of information gathering. It will examine some of the issues that arise from the regulatory framework within which this information gathering takes place. It will also address the issue of *instrumental clarity* and whether existing and new directives, requirements and approaches are sufficiently clear to enable reporting institutions on the 'front-line' to operate effectively.

The emergence of a new battleground

According to a number of authors (see [23, 33]), money laundering is not a modern phenomenon. Money laundering techniques were applied over 2000 years ago by the ancient Chinese merchants, who used various means, including purchasing movable assets and sending money abroad, to protect their wealth from the government (see [29]); by the moneylenders in the Middle Ages who invented various mechanisms to cover up their evasion of laws which criminalised usury [33]; by the pirates of the Mediterranean who deprived Rome of its supplies and concealed their loot but were eventually defeated by Pompey in 67 BC and the pirates who targeted European commercial vessels during the 16th–18th centuries and became "pioneers in the practice of laundering gold" ([33] p. 1).[2] Concealing one's wealth for tax evasion purposes is also an old phenomenon. Secret banking in Switzerland, for instance, dates back to at least the time of the French Revolution [27, 32]. However, even though tax evasion and money laundering techniques existed, the concept of money laundering, in terms of providing a legitimate appearance to ill-gotten gains, was yet to materialise. It was not until the early years of the 20th century, when the US tax authorities began to require proof of legal earnings, that the concept of money laundering became particularly relevant [2, 19]. There was also the emergence of 'organised crime' on the political agenda during the 1920s (see for relevant developments [19]). The fight against organised crime and the process of globalisation of economic and regulatory policies after the First and Second World Wars prepared the world for what became later a global war on money laundering. The war on money laundering and the related concept of following the money trail and hitting the criminals where it hurts most became a prelude to a global system of asset forfeiture.

The USA has undoubtedly been the main driving force behind the introduction of anti-money laundering regulations worldwide and the establishment of FIUs. The Financial Record-Keeping and Reporting of Currency and Foreign Transactions Act of 1970, known as the Bank Secrecy Act (BSA),[3] constituted the first comprehensive American anti-money laundering law. The Act did not explicitly contain the

[2] P. 1 of an online available pdf version
[3] 31 U.S.C.1051 et seq.

term ‘money laundering’ and neither did subsequent regulations of 1972[4] and of 1977.[5] However, the Act was introduced to target crime-money concealment and laundering, and, in the main, tax evasion. It stipulated that financial institutions maintain records and file reports so as to enable law enforcement authorities to track financial transactions in criminal, fiscal or regulatory investigations.

The term ‘money laundering’ can be traced back to 1973 when it appeared in print during the Watergate scandal [12[6], 18, 26]. The term was first used in a judicial context in 1982 in the case US v $4, 255, 625.39 (1982) 551 F Supp 314, and it subsequently spread worldwide [12].

The first US federal law to criminalize money laundering, the Money Laundering Control Act, was introduced in 1986. However, during the 1980s money laundering was still primarily associated with drug trafficking.[7] Two years after the introduction of the 1986 Act, on the eve of global economic liberalisation and just before the fall of the Berlin Wall, the international community reached agreement on two documents and these represented the first major steps towards international cooperation in the fight against money laundering. The two agreements in question were the UN Convention Against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances (Vienna Convention/19 December 1988) and the Basle Statement of Principles on the Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (December 1988).

The Basle Statement outlined several basic principles with regard to the banking system, including the need for customer identification and cooperation with law enforcement authorities. The Vienna Convention addressed the confiscation of assets and the issue of bank secrecy, and envisaged, *inter alia*, mutual legal assistance between Member States.

These agreements were hugely significant for the development of global anti-money laundering policies. However, they were not sufficient. The next step was to create an international forum that could be used to promote or, if necessary, impose policies worldwide. The Financial Action Task Force on Money Laundering (FATF) became this forum.

The FATF was established in July 1989 in Paris during the fifteenth annual Economic Summit of the G7, bringing together the US, Japan, Germany, France, UK, Italy and Canada. The summit participants also invited Sweden, Netherlands, Belgium, Luxembourg, Switzerland, Austria, Spain and Australia to join the Task Force. The FATF was created to help enhance international cooperation and assess the results of anti-money laundering policies globally. According to a 1996 report of the US General Accounting Office,[8] “the United States’ multilateral efforts to establish global anti-money-laundering policies occur mainly through FATF” [34]. The FATF also became instrumental in the efforts of the US to broadcast the ‘threat

[4] Sec. 103.23 Reports of transportation of currency and monetary instruments

[5] Sec. 103.24 Reports of foreign accounts

[6] Gillmore [12] makes a reference to Vallance, [36].

[7] The US Money Laundering Control Act of 1986 referred to proceeds from “specified unlawful activity” which, in addition to drug proceeds also included *inter alia* the proceeds of extortion, fraud and bribery. Nevertheless, for a number of years the focus remained largely on drug-related offences.

[8] The US General Accounting Office was renamed US Government Accountability Office (GAO) in 2004.

image' of organised crime (see [6], pp. 22–34). The FATF has directed the war on financial crime and money laundering by acting as an informal vehicle for enforcing US foreign policy in this field.

In 1990, the FATF issued a report describing the purported state of affairs concerning drugs money, and laid down forty recommendations.[9] The word 'recommendations', however, is misleading as these recommendations proved to be no less imperative than treaty obligations. Using the procedure of evaluating countries individually, the FATF turned its recommendations into an instrument of pressure: evaluated countries were to be listed as 'non-cooperative' unless they adopted FATF standards [7, 21, 24, 31]. In this way the FATF cemented the foundations of an unprecedented global anti-money laundering control system. It enforced a strategy that required financial institutions and other market players to become watchmen and report suspicious or unusual activities to "the competent authorities", i.e. to the frontline regiment of FIUs. The FATF has endorsed the position of FIUs on the frontline as the processor of intelligence and as a vehicle for intelligence dissemination between the reporting institutions and law enforcement/ regulatory agencies.

The drive for intelligence gathering

New battlegrounds require new forms of intelligence gathering. Naturally, on the money laundering front intelligence primarily concerns financial transactions and money flows. This drive for financial intelligence and the need to streamline efforts in information gathering and processing led to the establishment of the first FIUs. In some jurisdictions (primarily world financial centres) appropriate units, forerunners of the modern FIUs, were set up in the mid-to-late 1980s, at around the time of the introduction of relevant national anti-drug trafficking regulations as well as the Vienna Convention and the Basle Statement of Principles. For instance, the UK established the National Drugs Intelligence Unit (NDIU) in 1985. The NDIU[10] was assigned with the task of collecting disclosures concerning drug-related suspicious transactions from financial institutions and providing relevant intelligence to other investigative agencies (see [25]). The Isle of Man Financial Crime Unit became operational in 1986, while the Cayman Islands' Financial Reporting Authority (CAYFIN), and Hong Kong's Joint Financial Intelligence Unit (JFIU), both became operational in 1989. Guernsey's FIU, the Financial Intelligence Service, was formed in 1989. Australia founded its own FIU, the Australian Transaction Reports and Analysis Centre (AUSTRAC), in 1989 in accordance with the Financial Transaction Reports Act of 1988, and the unit began operating in January 1990. The American FIU, the Financial Crimes Enforcement Network (FinCEN), was established in April 1990.[11]

[9] The FATF revised its recommendations in 1996 and 2003, and additionally issued nine special recommendations on terrorist financing (eight in 2001, and one in 2004) as well as various "Interpretative Notes" to reflect developments in money laundering practices and to provide further guidance.

[10] For many years the UK's FIU was the National Criminal Intelligence Service (NCIS), which was formed out of the NDIU and set up as a separate body in 1992. In 2006 NCIS was merged into a newly created agency, Serious Organised Crime Agency (SOCA).

[11] I am grateful to the Egmont Group Secretariat for assisting me in confirming these dates.

Despite these early developments, the function of FIUs as central bodies responsible for money laundering compliance was yet to be determined and subsequently enforced and strengthened during the 1990s. FinCEN took the lead in establishing a global network of FIUs.

FinCEN was established to provide the US government with intelligence from multiple sources and the capabilities to analyse leads to help law enforcement agencies and prosecutors detect, investigate and prosecute financial crimes. FinCEN's duties broadened in the years following its establishment: in May 1994 its mission was expanded by the US Treasury to include regulatory responsibilities.[12] FinCEN's extended responsibilities included the following: promulgating regulations under the Bank Secrecy Act, evaluating BSA violations and recommending appropriate civil penalties, and providing assistance in leading the Treasury's efforts in fighting money laundering both inside the country and internationally [35]. This effectively meant that FinCEN was to take the lead role in expanding the intelligence drive outside the jurisdiction of the US by promoting the creation of similar units abroad. FinCEN set the example for the creation of a central national government facility that would not only play a crucial role in the sharing of information among law enforcement agencies and other regulatory partners, but would also gather and process intelligence from private sector organisations obliged to report any suspicious activity to FinCEN.

The need to appoint authorities specifically responsible for combating money laundering was highlighted by the 1990 Council of Europe Convention No 141 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 1991 EU Council Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering (91/308/EEC). Nevertheless, the establishment of FIUs during the early 1990s was viewed as "isolated phenomena related to the specific needs of those jurisdictions establishing them" (see [9], p. 3). It was not until the mid-1990s that FIUs were recognised on a much larger scale as a crucial part of anti-money laundering strategy. In 1995 several FIUs, including FinCEN, combined their efforts to develop a global forum for promoting the establishment of FIUs across the world. This forum, which became known as the *Egmont Group*, was founded as an informal organisation in Brussels on 9 June 1995. In 1996 the Egmont Group adopted a definition of FIU that was later incorporated in the revised FATF recommendations of 2003 and other international documents. Egmont Group defined FIU as:

> a central, national agency responsible for receiving (and, as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information:
>
> (i) concerning suspected proceeds of crime, or
> (ii) required by national legislation or regulation, in order to counter money laundering[13] ([9], p. 2).

Indeed the establishment of the Egmont Group signified a crucial turning point in the global fight against money laundering as it strengthened international

[12] In October 1994 FinCEN was merged with the Treasury Department's Office of Financial Enforcement (OFE) which had previously administered the BSA (see http://www.fincen.gov/helpfin.html).

[13] This definition was later expanded further to include terrorist financing.

cooperation and helped create better mechanisms for the cross-border exchange of information. This role of Egmont Group has been fostered by FinCEN in particular. On its website FinCEN States[14] that since 1995 "the U.S. has pursued an aggressive policy of promoting a worldwide network of Financial Intelligence Units in its overall strategy of fighting money laundering and terrorist financing." However, there were still setbacks to be overcome with regard to international intelligence sharing.

Initial setbacks in intelligence sharing

As authorities officially designated to receive reports of suspicious transactions, the FIUs have access to multiple sources of information that may help identify criminals and money launderers (some of whom are one and the same person). By sharing such information amongst themselves FIUs help fight money laundering on a global scope. However, apart from the obvious human rights and data protection limitations relating to such procedures, FIUs had at some point to address problems of cooperation resulting from the differing legal statuses of different types of FIUs.

The Egmont Group [9] defines the following types of FIUs:

- the *judicial type* (or prosecutorial, as defined by the IMF [15]) exists within the judicial branch of the state;
- the *law enforcement type* exists within the national law enforcement system;
- the *administrative type* is "a centralized, independent, administrative authority, which receives and processes information from the financial sector and transmits disclosures to judicial or law enforcement authorities for prosecution. It functions as a 'buffer' between the financial and the law enforcement communities" ([9], p. 3);
- the *hybrid type* combines elements of at least two FIU models (of those named above) and functions as an intelligence processing and disseminating body for the police and judicial authorities.

Each of these models has its advantages and disadvantages, but the main problem arising from having different types of FIUs worldwide is the variation in their competences. While a law enforcement type FIU may have broader or more significant investigative powers, an administrative type FIU runs the risk of turning into an intelligence collection depot that is used only to disseminate intelligence but has no analytical competence. On the other hand, administratively-geared FIUs appear to be more trusted by financial institutions as these are more likely to disclose information to a "neutral, technical, and specialized interlocutor" ([15], p. 11).

Differences in organisational forms of FIUs may hinder the exchange of information across borders. A report by the European Commission [4] highlights that such problems have indeed emerged: at some points FIUs of law enforcement type in certain Member States were only able to cooperate with similarly placed law enforcement counterparts.

[14] http://www.fincen.gov/int_fius.html

However, as a result of further legislative developments, particularly following the terrorist attacks of 11 September 2001, an increasing number of countries have introduced measures that allow their respective FIUs to share information with other FIUs, even if they are of a different type [15]. In some instances problems relating to information sharing have been overcome through memorandums of understanding (MOU). The MOU has been designed by Egmont Group as a set of principles for information exchange based on reciprocity and only for the purposes of analysis at FIU level, with no further use allowed without the prior consent of the FIU that provided the information.

Clearly the drive for intelligence and the need to address the money-laundering phenomenon on a global scale requires effective cooperation between the various FIUs. However, the fact that FIUs differ in their organisational form may imply that countries address problems relating to money laundering in different ways. In order to prevent such lack of global consistency policy makers have sought to introduce a range of international requirements. These requirements were promoted and enforced through the aforementioned FATF recommendations (including subsequent revisions and interpretative notes), the 1990 Council of Europe Convention, the 1991 EU Council Directive (91/308/EEC) and its subsequent amendments (Second Directive of 2001[15] and Third Directive of 2005[16]). The issues that arise from some of these requirements, specifically those envisaged by the Third Directive, and how they affect the reporting system, are discussed in the following section.[17]

Strengthening strategy

Extending the outreach of anti-money laundering measures

Over the years changes in the strategy for the war against money laundering have led to the broadening of the scope of FIU-work and expanding the outreach of anti-money laundering measures. Whereas originally money laundering was associated primarily with illicit drug trade, the list of predicate crimes came to include practically all types of crimes-for-profit[18] (with some exceptions in various countries).

Additionally, the group of entities obliged to report suspicious transactions significantly expanded over the years to include not just classical financial service

[15] 2001/97/EC

[16] 2005/60/EC

[17] Although the EU Directive applies specifically to EU Member States, other countries where similar regulations have been introduced face similar challenges as those arising from the EU Directive.

[18] The 1990 Council of Europe Convention expanded the definition of money laundering beyond that laid down by the 1988 UN Convention, which defined laundering in association with drug-related offences only. The Council of Europe Convention describes the underlying criminal activity that generates the money subject to subsequent laundering as a "predicate offence" (see [12], for an account of international legislative developments).

institutions, but also casinos, brokerage and securities firms, lawyers, notaries, auditors, real estate agents and so on.[19]

These changes have resulted in the extension of the outreach of anti-money laundering measures, which policy makers believe will help prevent the corruption of the financial system; and this has itself been underpinned by the broad definition of money laundering. At the outset of the fight against money laundering the concept of money laundering was broadened to include practically every act that is subsequent to profit-seeking crime [7, 30]. By overstretching the meaning of money laundering, to cover the movement and concealment of crime money, policy makers have effectively created a tool for gathering intelligence about predicate crimes [13]. The issue is whether this tool is being used efficiently considering the lack of precise criteria for discerning tainted money and suspicious or unusual transactions, in addition to the lack of consistent feedback from FIUs to reporting institutions.

Indeed government agencies, often jointly with industry associations, seek to provide guidance[20] (in the form of handbooks and typologies) to reporting institutions. However, in some cases this guidance remains broad, and, in certain respects, impractical. Staff within reporting institutions are expected to competently interpret relevant guidelines and be on the alert at all times.

Authorities and industry organisations in the UK have been particularly proactive in providing advice and guidance to the industry on matters relating to anti-money laundering control. In 2006 the UK Joint Money Laundering Steering Group (JMLSG)[21] produced a comprehensive guidance manual (updated in 2007)[22] that provides examples of high-risk customers and suspicious transactions. Examples include: corporate customers with complex business ownership structures; politically exposed persons; customers based in or doing business in high-risk jurisdictions; customers engaged in cash-intensive businesses; the use of non-resident companies in circumstances where the customer's needs do not appear to support such economic requirements; transfers to and from high-risk jurisdictions without reasonable explanation; and unusual investment transactions without an apparently discernible profitable motive. Examples of transactions that could trigger suspicion

[19] Following the Money Laundering Control Act of 1986 the US government introduced a number of additional federal statutes and regulations that significantly expanded the list of reporting institutions and ensured that certain groups of organisations outside the banking system were also subject to formal reporting requirements. For instance, the Money Laundering Suppression Act of 1994 imposed more rigid reporting requirements on non-banking financial institutions (e.g. brokerage companies, some tribal casinos etc), which prior to that point had been largely unregulated. Gradually, the US approach to extending the list of reporting institutions was adopted globally.

[20] The FATF, the Basel Committee and other international bodies have also issued guidance at various points on know-your-customer rules and risk management.

[21] An industry organisation (comprising a number of financial sector trade bodies) engaged in providing advisory services on compliance with legal and regulatory requirements and good practice.

[22] An updated version of this manual was issued in December 2007. The guidance was issued in two parts: a) Guidance for the UK Financial Sector, Part I, b) Guidance for the UK Financial Sector, Part II: Sectoral Guidance (Joint Money Laundering Steering Group, December 2007; available on the JMLSG website – http://www.jmlsg.org.uk).

in relation to terrorism include frequent international ATM[23] (cash machine) activity. The authors of this guidance manual have endeavoured to compile a methodical set of requirements and, more importantly, instructions on how to implement them.

However, although these examples may be useful as general guidance, some of them remain vague: for instance, almost any customer from Eastern Europe, Russia or the Middle East could be regarded as a potential risk factor, irrespective of the type of transactions they undertake.[24] The *risk* of money laundering is in itself an unclear concept. Does it relate only to a specific transaction (as more commonly understood) or generally to a customer and his/her activities? The manual interchangeably refers to (a) knowledge or suspicion that a *transaction* might involve money laundering; and (b) knowledge or suspicion that a *customer* might be involved in money laundering, which is not quite the same thing. Furthermore, money laundering is such a broad concept that even marginal irregularity may trigger suspicion, and suspicion prompts reporting to the relevant FIU. Suspicion, however, is also a malleable term, a variable that depends on different mindsets, subjective judgement and interpretation. The JMLSG admits that suspicion is indeed subjective and "falls short of proof based on firm evidence" ([16], p. 121). JMLSG's handbook notes that UK courts have defined 'suspicion' as something beyond mere speculation, and based on some foundation, for example: "A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not"; and "Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation" (p. 121). On its website the UK Serious Organised Crime Agency (SOCA), which incorporates the UK FIU, refers to R v Da Silva [2006] All ER (D) 131 (Jul) in which the Court decided that suspicion would arise when: "there was a possibility which was more than fanciful, that the relevant facts existed. This is subject in an appropriate case, to the further requirement that the suspicion so formed should be of a settled nature."[25] Although the clarification provided by JMLSG and SOCA is helpful, it remains broad and leaves scope for interpretation.

The JMLSG insists that firms should encourage their staff to "think risk" ([16], p. 9) in appealing to basic human virtues such as common sense, intelligence and motivation. However, while the commitment and care of individual staff members are of significant importance, the demand and need for 'quality intelligence' also requires a clear basis for developing shared standards that ensures optimal objectivity and consistency in decision-making.

Additionally, although UK authorities have indeed actively assisted the industry by providing advice and detailed guidance, ensuring consistency of approach and the

[23] Automated teller machine

[24] As an example of poor practice and lack of a "robust approach to classifying the money laundering risk associated" with clients, the UK's financial regulator, the Financial Services Authority (FSA), drew attention to a wholesale small firm that classified all of its clients as low or medium risk even though most of them were based in Eastern Europe, North Africa and the Middle East ([10], p.12).

[25] SOCA notes that in K Limited v National Westminster Bank plc (HMRC and SOCA intervening) [2006] All ER (D) 131 (Jul) the Court has decided that this definition should apply in both criminal and civil cases. See http://www.soca.gov.uk/financialIntel/faqs.html.

enforcement of respective national regulations throughout various countries remains a pressing issue.

Expanding target to include financing of terrorism

After the events of 11 September 2001 the criteria for reporting suspicious transactions have been expanded to include transactions that may be linked to terrorist financing. The Third Directive places particular emphasis on this issue. This means that reporting institutions are now obliged to keep a look out for clean money that may serve terrorists in addition to potentially dirty money.[26] However, it is not quite clear how reporting institutions are supposed to be able to identify such risks. The situation varies across countries, but in general terms little or no specific guidance has been given as to how to determine whether or not a customer or a partner may be linked to or involved in terrorist financing. Is running the names of clients through databases of national and international blacklists and sanctions lists sufficient? Should banks and other reporting institutions watch out for connections to 'countries of risk'? For instance, if a European bank is conducting a due diligence[27] exercise on a potential client in Ukraine, should the bank also seek to understand whether their Ukrainian client has ever done business in any of the countries that may be deemed as 'risky', e.g. Iran, Iraq, North Korea, Libya? If such links exist, should the reporting institution be concerned and should they notify the relevant FIU? It seems that the approach to be adopted in this matter is largely to be defined by the reporting institutions themselves on a discretionary basis. Due to the lack of clearer guidance and criteria for discerning suspicious activity (both with regard to suspicion of money laundering and terrorist financing), particular ethnic or national groups could potentially become targets of systemic suspicion and scrutiny (see [13]). If the reporting institutions had clearer guidance on this matter, they could prove a useful source of targeted intelligence. The Directive does indeed require Member States to provide access to up-to-date information on the practices of money launderers and terrorist financers and on indicators leading to the identification of suspicious transactions (Article 35.2). The question remains, however, how clear these indicators are and how consistently they are applied across various sectors and countries.

Politically exposed persons

Additional challenges for reporting institutions and the authorities exercising anti-money laundering control may arise from the implementation of the requirement of the Third EU Directive in relation to the identification of Politically Exposed

[26] For instance, in some circumstances charities can be used as a front for (or vehicle of) terrorist financing: banks that carry out financial transactions involving or on behalf of charities may find themselves in a situation which necessitates that they report to the relevant FIU; however, banks may overlook important underlying risks due to the lack of sufficient and clear guidance in existing regulations.

[27] The term 'due diligence' is generally understood as the use of procedures aimed at verifying the identity of a customer or a potential business partner. The meaning of the term, however, has gradually been broadened to denote a process of enhanced due diligence meaning examining the background, integrity, sources of wealth, extent of political exposure, and so on, of a customer, a potential business partner or an investment target.

Persons or PEPs. Once again reporting institutions are expected to be the source of intelligence that the authorities would otherwise have difficulties in gathering. Background checks aimed at identifying PEPs appear to be a good way of gathering intelligence about potential tax evasion and white-collar crime.

According to the Directive (Article 3 (8)), PEPs are "natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons" (*Official Journal of the European Union*, 25.11.2005, p. 22). The Directive stipulates the necessity of "enhanced due diligence", or, in other words, "rigorous customer identification and verification procedures", in cases of non-domestic PEPs, i.e. individuals who hold or have held "important public positions" in another Member State or a third country, particularly in countries where corruption is endemic. With regard to domestic PEPs, reporting institutions are advised to apply "complete normal customer due diligence measures" (or "simplified due diligence",[28] for instance, with regard to customers entrusted with public functions in accordance with the Treaty on European Union). However, it is not explicitly clear whether identity verification on its own is satisfactory in meeting the requirement for "complete normal customer due diligence" or whether it should be combined with other measures.[29] Article 8 of the Third Directive stipulates that customer due diligence measures comprise the following: identifying the customer and verifying his/her identity on the basis of information from a reliable and independent source; obtaining information on the purpose and nature of any given business relationship; monitoring of business relationships, including, where necessary, source of funds. Article 13 defines enhanced customer due diligence as the measures listed in Article 8 in addition to measures that include establishing the source of wealth of non-domestic PEPs and/or gathering information on the reputation of respondent institutions and assessing their anti-money laundering control systems. If the prescribed "complete normal customer due diligence measures" implies the necessity of establishing and verifying the identity of any given customer, it remains unclear how far beyond that point reporting institutions should go in applying "enhanced due diligence measures". The scope of due diligence work undertaken with regard to non-domestic PEPs is, therefore, to be decided by individual reporting institutions.

[28] The Directive appears to distinguish three levels of due diligence: 1) standard or normal customer due diligence which includes identity verification and understanding of the nature of the customer's business; 2) enhanced due diligence in situations of heightened risk where additional information should be gathered; 3) simplified customer due diligence where the situation does not necessitate identity verification. In the latter case, the Directive envisages that by way of derogation Member States may allow reporting institutions not to apply customer due diligence procedures in certain situations, for instance in the case of listed companies in Member States or clients with life insurance policies where the annual premium is no more than € 1.000 (in any event, reporting institutions need to gather sufficient information to establish whether the customer qualifies for an exemption). From the text of the Directive (Article 7) it also appears that occasional transactions amounting to less than € 15.000, that are not associated with any knowledge or suspicion of money laundering or terrorist financing, may also in certain situations be subject to simplified know-your-customer rules.

[29] The aforementioned JMLSG manual contains a checklist for standard evidence that should be obtained by the reporting institutions with regard to various types of customers. However, as mentioned elsewhere, although authorities in the UK have endeavoured to provide detailed guidance to the industry, ensuring consistency of approach throughout various countries remains an unresolved issue.

In addition to this, the precise meaning of "important public positions" and "prominent public functions" also remains ambiguous. Furthermore, it may prove difficult in establishing whether a customer is an immediate family member or a close associate of a PEP unless the customer explicitly declares that such a relationship exists.

In an attempt to clarify these issues, the European Commission has issued a set of implementing measures[30] according to which only public functions exercised by a customer at a national level are regarded as "prominent". It is further stipulated that where the extent of political exposure at lower (i.e. local) levels is comparable to similar positions at the national level, it is at the discretion of the reporting institutions to decide, depending on the level of risk (on a "risk-sensitive basis", a concept discussed in an another section of this paper), whether or not these individuals should be regarded as PEPs. It appears that this guidance rests on the assumption that reporting institutions have some prior knowledge of existing political structures in the country of origin of their customer(s), which is not necessarily always the case. In an effort to provide guidance to reporting institutions the European Commission has provided[31] an instructive checklist for PEP figures; and it has also indicated that middle ranking and junior officials are to be excluded from the PEP category. This may well have made things slightly easier but not significantly clearer. If the purpose of identifying PEPs is to become aware of the possibility that they may become involved in corrupt practices — i.e. that they represent a laundering-risk factor — it is not clear why junior or regional level public posts are excluded from the PEP category. Perhaps it is assumed that the more central the role of the PEP in national politics, the larger the scope of potential corruption and reputational risk associated with the PEP's role. This, however, is not necessarily always the case.

Furthermore according to the EU Directive, risk is generally higher in countries where corruption is widespread. Once again the European Commission assumes that reporting institutions have existing knowledge about the political environment in the countries of residence of their customers. However, in order to be able to identify countries of heightened risk, reporting institutions are likely to rely on external criteria and surveys such as the Transparency International Corruption Perceptions Index and/or reports produced by the Economist Intelligence Unit, and these may not necessarily suffice as supplementary material for their specific purposes. According to Séverine Anciberro, a representative of the European Banking Federation, the EU should be considered a single jurisdiction and PEPs from EU Member States should be regarded as domestic PEPs because credit institutions in Member States are already implementing relevant due diligence procedures [1]. Anciberro notes that the banks in Europe would have preferred if PEPs were regarded as a risk factor only in cases where transactions were particularly substantial or complex in nature, thereby

[30] COMMISSION DIRECTIVE 2006/70/EC of 1 August 2006 "laying down implementing measures for the 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" (*Official Journal of the European Union* L 214/29 – L 214/34, 4.8.2006).

[31] COMMISSION DIRECTIVE 2006/70/EC

posing enhanced money laundering and reputational risks. Such an approach would necessitate the undertaking of enhanced due diligence investigations only in circumstances where PEPs appear to have engaged in potentially suspicious transactions. The Federation's proposal, however, was not adopted.

The EU Directive presents further challenges. If a reporting institution is aware that a customer is a PEP residing in another country, clearly the institution in question will be obliged to undertake, on a risk-sensitive basis, an enhanced due diligence investigation into the integrity and background of this customer. But what happens if the institution is not immediately aware of particular public or prominent roles occupied by their customer? Article 13.4(a) of the Third Directive states that "in respect of transactions or business relationships with politically exposed persons residing in another Member State or a third country, Member States shall require those institutions and persons covered by this Directive to: (a) have appropriate risk-based procedures to determine whether the customer is a politically exposed person [. . .]" (*Official Journal of the European Union*, 25.11.2005, p. 25). This provision leaves scope for interpretation to the extent that reporting institutions will be obliged to run checks on any customer(s)[32] residing in other Member States or third countries to determine whether they are in fact PEPs. This means that standard or "complete normal" due diligence measures undertaken on customers living in another country could probably never be completely adequate. Even in situations where reporting institutions are well acquainted with the political environment of a specific country, and the associated risks, establishing the identity of the customer would not be sufficient in establishing whether or not the customer is also a PEP. In such circumstances there are two possible options: (a) the customer would have to either declare any public positions held or (b) additional research would be undertaken by the reporting institution into the profile of the subject. This means that in order to identify whether a customer is a PEP, the reporting institution is obliged to conduct enhanced due diligence. The same applies to close associates of PEPs.[33] However, the implementing measures directive (Commission Directive 2006/70/EC) states that the requirement of institutions to identify close associates of PEPs (in accordance with Directive 2005/60/EC) applies to the extent that the relation between the PEP and their associate is publicly known or that the institution has reasons to believe that such relation exists. The European Commission further notes that this does not presuppose active research. Yet if a customer from Nigeria applies for an investment loan in London, bank officers are not necessarily aware of the public role, if any, of the customer in Nigeria or whether the subject is a close associate of a high ranking political official. It is clear that in such cases establishing

[32] Except for situations where, as envisaged by the EU Directive, simplified-know-your-customer rules (explained earlier) may be applied.

[33] Article 2, paragraph 3 of the implementing measures directive (Directive 2006/70/EC) stipulates that 'persons known to be close associates' shall include: a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP; b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP. Thus formulated, this article leaves scope for interpretation to the extent that the category of associates of PEPs can also include other groups of individuals who are linked to PEPs.

the identity of the customer is not sufficient and that more in-depth background checks would have to be undertaken.

Furthermore, with regard to PEPs in other Member States or third countries, Article 13 of the Third Directive requires reporting institutions to take adequate measures to establish the source of wealth and source of funds involved in any given business relationship or transaction. In practice this translates into, first, establishing whether or not a customer is a PEP; and, second, undertaking further research in order to ascertain the legitimate origin of the PEP's funds, which is something that even the police and tax authorities may have difficulty ascertaining.

Article 13 of the Directive states that enhanced customer due diligence measures must be applied in situations which by their nature can present a higher risk of money laundering or terrorist financing. Reporting institutions should regard relationships with PEPs from other countries as a higher risk factor in any case, although the precise definition of 'higher risk', and the scope of the relevant enhanced due diligence checks, are to be determined by individual reporting institutions.

It should be noted that for a number of years, preceding the introduction of the Third Directive, due diligence checks have often been aimed at establishing whether an individual might be politically exposed or linked to organised crime. In many cases, particularly in Europe, this has been done as a matter of good risk management practice and not necessarily in a bid to comply with specific regulations. The concept of political exposure implies a range of risks, which are not limited to potential involvement in corruption and/or money laundering, and also include political and other, ultimately reputational, risks. The reputation or business standing of an individual or a business may be harmed as a result of political confrontation, for instance. This point is particularly valid in terms of emerging markets where business and politics remain closely intertwined. The extent of such political exposure and the associated risks does not solely depend on whether an individual holds a public position of authority. Political exposure may additionally arise from party affiliations or business associations.

Such assessments undoubtedly require proactive research and enhanced due diligence measures. According to a study undertaken by KPMG in 2007, in 2004 45% of banks reported that they had special procedures in place for identifying and monitoring PEPs, whereas in 2007 the figure increased to 71%. In the US, however, nearly all banks introduced such procedures in compliance with the U.S.A. PATRIOT Act of 2001. KPMG's study also notes that banks are increasingly using independent due diligence providers to verify the identity of their clients [17]. However, the due diligence industry now appears to be driven more by legislation rather than by a desire for sound risk management practices. Furthermore, it is difficult to discern whether some institutions are conducting work diligently or whether research is being taken to excessive extremes as there is a definite lack of consistency. Of more importance: there is no effective evaluation of due diligence procedures across economic sectors and jurisdictions (even within the European Union).

Due to the general fuzziness of criteria and guidelines for due diligence reporting, FIUs and their regulatory partners are unlikely to be receiving the quality intelligence from reporting institutions that they expect. This is true, for instance, in terms of due diligence investigations in investment and private banking where the

risk of money laundering can be relatively high. Almost any customer from an emerging market associated with/or a PEP[34] can be regarded as a potential money launderer. Nevertheless, in the absence of clearer criteria, it seems that financial and non-financial service providers alike are happy to work with PEPs and their associates as long as these are wealthy individuals and do not look like outright criminals. Whether or not these subjects have a controversial reputation is a subjective point. This is only directly relevant to reporting institutions in so far as to ensure that they do not incur financial losses either as a result of reputational damage or penalties.

Banks certainly need to be aware of the potential transaction risks, political risks, reputational risks and so on that may be associated with a specific customer. Yet it is not explicitly clear whether and when an existing risk, specifically money laundering/terrorist financing risks (which also fall into the category of reputational risks), becomes a deal-breaker and, more importantly, a reason for reporting to the relevant FIU. The fact that a potential risk exists does not mean *per se* that the transaction is suspicious or that the customer is a money launderer. It is difficult to make judgements and to strike balances. It is often the case that even within one single institution different departments view risks in different ways. While compliance departments anxiously seek to identify potential areas of reputational concern associated with their clients, officers on the banking or marketing side sometimes tend to be less concerned about reputational issues or else view them as unsubstantiated. And to an extent they have a point especially because it is often difficult to verify or prove reputational concerns, particularly when they are based on rumours. Should a transaction be reported by a compliance officer to the relevant FIU in instances where due diligence checks have uncovered integrity suspicions based on rumours only? A bank may decide not to proceed with a specific deal because of rumour-related concerns but it is not explicitly clear whether that information should be fed into the general flow of intelligence to the relevant authorities. Presumably there would be no need to file a report if the reasons for concern were regarded as mere speculation. But, again, there is scope for interpretation on this point.

[34] The implementing measures directive (2006/70/EC) clarifies that after an individual has ceased to exercise a prominent public function, subject to a minimum period, this individual is no longer to be regarded as a PEP (point 5 of the introduction). The directive further stipulates that "without prejudice to the application, on a risk-sensitive basis, of enhanced due diligence measures, where a person has ceased to be entrusted with a prominent public function [. . .] for a period of at least one year, institutions [. . .] shall not be obliged to consider such a person as politically exposed" (Article 2, paragraph 4, p.32). However, this can be interpreted to the extent that in certain circumstances, on a risk-sensitive basis, some individuals should be regarded as PEPs even after a year has elapsed since ceasing to hold a prominent public function. As mentioned elsewhere in this paper, in emerging markets politics and business are not completely divorced. Successful businessmen, including former politicians that have embarked on developing careers in private business, often forge some sort of a business arrangement with current politicians, i.e. PEPs, in order to ensure support for their own interests. This suggests that former politicians and/or legislators turned businessmen are also to be regarded as PEPs in certain circumstances on a risk-sensitive basis.

The general practice shows that, albeit somewhat ironically, over the years criminal or tainted money has undergone a process of evolutionary cleansing and purification. A majority of today's tycoons, including those known and less well-known wealthy businessmen from former Socialist countries, made their fortunes in the early years of market reform and economic liberalisation when business practices were highly questionable, if not outright criminal. Yet these very same businessmen, many of whom later became categorised as PEP(s), are now transforming the reputations of their businesses and demanding to be viewed as legitimate players. The growth of business requires new forms of business relationships, with lenders, co-investors, IPO[35] underwriters and advisors, which inevitably leads to higher public exposure, hence the need for more transparency. As Savona [28] notes, criminal organisations need to "develop an aura of respectability" (p. 8) and legitimise themselves if they want to ensure the unfettered circulation of their capital. Such evolutionary processes have taken place not just in the former Socialist bloc but also in other parts of the world, including the USA [28].

The important question is whether the wealth of newly defined 'legitimate' businessmen, including in some instances PEPs or those formerly involved in questionable activities, is still in some way tainted. But this remains a question with an unclear answer and a wide array of implications, including moral, economic and legal.

Relationships between financial and other reporting institutions with non-domestic PEPs remains a sensitive issue that can have legal consequences not simply under anti-money laundering regulations but also under the US Foreign Corrupt Practices Act (FCPA),[36] where there is involvement of US institutions. For US institutions that hold potentially guilty knowledge of questionable business practices involving PEPs possible implications include penalties and reputational damage.

The existing anti-money laundering control procedures are designed in a way that inevitably provokes fear of penalties and reputational damage. However, this fear does not automatically mean that reporting institutions will provide higher quality intelligence to the authorities in a consistent and methodical way, because the system is largely based on vague concepts and subjective assessments. Extra-systemic and unforeseen procedures including whistle blowing, for instance, can prove effective in correcting misconduct by reporting institutions, such as, for instance, the concealment of culpable knowledge of factors of suspicion by

[35] Initial Public Offering or the flotation of a private company on a stock market, i.e. a company's first offering of shares to the public.

[36] The FCPA was enacted in 1977. Gradually other countries followed suit and introduced similar regulations. In 1997 the OECD adopted its Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, which came into force in 1999.

reporting institutions. But even such instances do not ensure the necessary flow of useful intelligence.

Beneficial owners and correspondent banking relationships

Another challenge posed by the Third Directive arises from the requirement to identify beneficial owners, i.e. the individual wielding ultimate control over the customer and/or the individual or entity on whose behalf a transaction is conducted. The Directive defines beneficial owners as holding 25% or more of the shares in a business. Good risk management and reputational checks practices conform to this requirement in any event but in some cases it might be impossible to identify the ultimate owner. European banks have expressed their concern that banks do not always have access to trustworthy sources of information that would allow such identification [1].

Banks have also stressed that another challenge posed by the Directive is the requirement that they do not engage in correspondent relationships with banks known for allowing their accounts to be used by a shell bank(s). In this respect Anciberro [1] notes that the obligation to know the customer's customer is generally not workable.

The Directive lays down these requirements without providing any practical guidance as to how they are to be implemented. It appears that in both cases — the identification of beneficial owners and verification of correspondent relationships — reporting institutions would need to implement enhanced due diligence procedures but, once again, the scope of these must be determined by individual reporting institutions. More often than not banks and other reporting institutions resort to using the services of independent due diligence providers to ascertain the true ownership of a company/establish whether a correspondent bank is engaged in relationships with obscure banks. The key question is at what point and under what circumstances does the gathered information become useful intelligence for regulators.

Risk-based approach: another ambiguous concept?

The central message of the Third Directive is two-fold in its call for a) enhanced customer due diligence in all situations where there is a higher risk of money laundering and/or terrorist financing; and b) the implementation of adequate measures to compensate for the higher level of risk in situations in which the customer has not been physically present for identification purposes. An important amendment introduced by the Third Directive affecting the anti-money laundering control system is the introduction of a risk-based approach. The Directive asserts that enhanced due diligence will be applied on "a risk-sensitive basis". This means that reporting institutions can decide for themselves when and in what circumstances to undertake in-depth due diligence checks. To this end, reporting institutions should have clear direction and criteria on deciding which customers are "high-risk". Having said that, on the basis of the Directive it appears that non-domestic PEPs and their sources of wealth, as well as correspondent banking relationships with respondent institutions from third

countries, should always be subject to enhanced due diligence regardless of whether reporting entities consider them 'low-risk' or 'high-risk'. The most important thing to remember, within the remits of the risk-based approach, is that reporting institutions should know precisely whom they are dealing with (e.g. to know the customer's identity, nature of business, place of employment and sources of funds, and so on), and, depending on the level of risk, decide the scope of due diligence for themselves.

On the whole the banking industry has welcomed the introduction of the risk-based approach as prescribed in the Third Directive [1]. In fact, the European Commission [3] has admitted that even prior to the introduction of the Third Directive many institutions had been applying a risk-based approach in non-face to face identification procedures. The risk-based approach helps to better focus resources besides circumventing the occurrence of costs that are not commensurate with actual risks.

The risk-based approach is fast becoming increasingly important in the USA as well. According to FinCEN's director, James Freis, "matching risk-based examination to risk-based obligations" would help achieve regulatory efficiency. Freis admits that a risk-based reduction in covered entities would lead to a more efficient concentration of examination resources [11].

It appears that prior to the introduction of the Third Directive (and similar regulations in countries outside the EU) nearly all changes in the strategy of the anti-money laundering war have led to over-regulation and over-compliance without achieving any evident success in the reduction of purported money laundering activities. Tables 1 and 2 (below) clearly show that the overall number of suspicious transactions reports submitted to the FIUs of several countries has increased over the years, specifically since 1994 (in some instances peaking in 2002 following the terrorist attacks of 2001). According to Scott McClain, Deputy General Counsel to the Financial Service Centers of America, money service businesses (MSBs) bear the cost of the US BSA enforcement strategy. He further adds that compliance with SAR[37] and CTR[38] requirements in the US has led to direct and substantial costs not just in the MSB industry but also across the whole financial services sector. These costs in turn have resulted into a pressure to increase fees charged to customers. McClain makes the point that existing regulatory pressures and the lack of clear guidance have ultimately led to a large number of defensive SAR filings as well as duplicative CTR filings. The level of suspicious transaction reports, according to McClain, clearly places a burden on government agencies, specifically FinCEN, which processes a large amount of data of "dubious value" as a result. In particular, McClain points out that the increase in regulatory scrutiny following the events of 11 September 2001 has led to defensive SAR filings that report even marginally irregular activity [22].

[37] Acronym for "Suspicious activity report"

[38] Acronym for "Currency transaction report"

Table 1 Number of suspicious activity report filings by year in some European countries

State	1994	1995	1996	1997	2002	2003	2004	2005	2006
Belgium	2.183	3.926	5.771	7.747	13.120	9.953	11.234	10.148	9.938
Germany[b]	3.282	2.935	3.289		8.261	6.602	8.062	8.241	10.051
France	684	866	902	1.213	8.719	9.019	10.842	11.553	12.047
Netherlands	14.753	15.007	16.087	17.000	137.339	177.157	174.835	181.623	-
-unusual	3.546	2.994	2.572		24.741	37.748	41.003	38.481	
-suspicious									
United Kingdom	15.007	13.170	16.125	14.148	56.023[a]	94.718[a]	154.536[a]	195.702	213.561

All figures in this paper are in Continental European annotation.
Source for figures relating to years 1994 to 1997: European Commission [4]
Source for figures relating to years 2002 to 2006: FIU's Annual Report(s)
[a] Source: [8]
[b] The 2004 annual report of Bundeskriminalamt, Germany's FIU, provides the following figures: 1994 — 2.873, 1995 — 2.759, 1996 — 3.019, 1997 — 3.137.

Table 2 Number of suspicious activity report filings by year in the USA

Institution	1996	1997	1998	1999	2000	2001
Depository Institution	62.388	81.197	96.521	120.505	162.720	203.538
Money Services Business	-	-	-	-	-	-
Casinos and Card Clubs	85	45	557	436	464	1.377
Securities & Futures Industries	-	-	-	-	-	-
Subtotal	62.473	81.242	97.078	120.941	163.184	204.915

Institution	2002	2003	2004	2005	2006
Depository Institution	273.823	288.343	381.671	522.655	567.080
Money Services Business	5.723	209.512	296.284	383.567	496.400
Casinos and Card Clubs	1.827	5.095	5.754	6.072	7.285
Securities & Futures Industries	-	4.267	5.705	6.936	8.129
Subtotal	281.373	507.217	689.414	919.230	1.078.894

Source: FinCEN, The SAR Activity Review — By the Numbers (Issue 9, January 2008)

As these tables illustrate, the number of suspicious transaction reports has increased over the years. This, however, does not necessarily mean that the quality of reports has improved. Policy makers hope that the risk-based approach will help reduce the number of poor quality reports and improve the quality of intelligence provided to FIUs. Nevertheless, the question of how to identify risks remains. Ambiguous terminology and the lack of systematic feedback from the authorities and FIUs to the reporting institutions are the main setbacks in the process of intelligence gathering. In the absence of clearer criteria, risk assessment appears to be largely based on the hunches, and in some cases tenacity, of individual researchers. Moreover, within the remits of a risk-based approach there exists a 'reverse risk': the risk of being wrong or, in statistical terms, the possibility of false positive and false negative errors. Risk-based decision-making in the absence of solid and precise definitions can be indeed a risky undertaking in itself.

The new turn in strategy — with the introduction of a risk-based approach to due diligence and intelligence gathering — may well prove critical in pre-empting unnecessary, ineffective and costly work. However, it is also an admission that anti-money laundering policies have been flawed somewhere along the line. Yet policy makers insist that the new change of tactic and strategy will result in victory. We have heard that before.

Conclusion: can we learn lessons from the past, at last, or will we revert to the old practices?

What is increasingly important now is for FIUs and other law enforcement agencies to create a more efficient way of feeding information back to reporting institutions. Otherwise the long awaited victory against money laundering will remain a fanciful and distant aim. Besides, perhaps it is time to start thinking about money laundering as the Achilles heel of criminal activity by which offenders can be identified. On the basis of reports on suspicious money laundering transactions FIUs can actually identify leads to predicate crimes. However, this can only be ensured by a system that is well designed and equipped to spot such transactions, as reporting institutions cannot be expected to act as spies or detectives. The system as it stands now is far from ideal. One can only speculate as to how much of the information that reporting institutions gather on their customers is actually used by FIUs. There are massive flows of reports about suspicious transactions, but how many of these are of good quality remains an issue. In addition, in the absence of proper definitions of 'suspicion' and 'risk', it is likely that substantial amounts of quality intelligence remains in-house and is never passed onto the relevant FIUs.

The introduction of the risk-based approach may prove a sensible move, provided that reporting institutions will receive systematic feedback from the respective FIU and clearer guidance on how to determine risk factors and how far they should go in their efforts to gather intelligence on their customers. It is also unclear what the implications of the risk-based approach would be if a PEP or another risk factor slips through the system. Should banks be held accountable for such failures?[39] It would be difficult to criticise a compliance officer for making an erroneous judgment when there is little consistency in defining 'suspicion'. In fact, it may be difficult to prove in a criminal context that a banker had doubts about a transaction but chose to ignore it [20]. Of course, law enforcement authorities may always find a reason to impose a penalty but such punitive actions do not necessarily result in quality intelligence. In fact, this can again lead to over-compliance in the form of over-reporting, which is precisely what the risk-based approach aims to prevent.

[39] For instance, the JMLSG handbook, reviewed earlier, notes that the FSA is unlikely to take enforcement action if a firm demonstrates that it has put in place an effective system of controls. But what essentially "an effective system" means is unclear. The guide uses broad terms such as "reasonable care", "reasonable steps", "appropriate steps", "appropriate procedures" etc., which fall short of explicitly defining the minimum prescribed standard that would guarantee defence against enforcement action.

From the perspective of individual FIUs, the increasing number of reports does not mean an improvement in quality. FIUs are unique 'knowledge centres' ([5], p. 67). They gather knowledge from organisations that are largely profit-oriented, and therefore it goes against the nature of these organisations to play detectives. In establishing an optimal suspicion threshold it would be helpful, therefore, to develop basic prescribed standards and automated knowledge-based systems, or artificial intelligence networks [13], in order to minimise the margin of subjective judgement. Besides, it is important to ensure that the guidance provided by the respective national authorities and the enforcement of regulations are consistent across countries.

There is a need for further clarity in the use of terms, especially now with the introduction of the risk-based approach. While risk is in itself a nebulous concept, the consequences of a risk-based approach and, more importantly, of its failures, are also unclear. Are the authorities being responsible enough by introducing a new approach that is based on such a fragmented foundation? Risk factors such as money laundering, corruption and terrorist financing remain highly nebulous for as long as there are no clear indicators in terms of the basis on which to act in order to minimise the risks of wrong decision-making and any resultant repercussions. The potential implications of ill-informed decision-making, in addition to the omission of vital information gathered, can range from reputational damage, which can result in substantial financial losses, to regulatory reprimand and fines. Little attention has been paid as to the practical side of how to strike a balance between the profit-oriented nature of the reporting institutions, the need to keep the financial system clean, and the fear of being punished by regulators. Until further clarity is achieved, there is a chance that the risk-based approach may at any time slide back to over-compliance as reporting institutions will wish to avoid the really feared risk of being reprimanded by the regulatory authorities (see [14]).

Reporting institutions need to be better informed to understand the rationale behind certain official requirements if they are to effectively apply a risk-based approach. It may be a 'war', but although reporting institutions find themselves on the frontline of this war, they do not necessarily make good soldiers, especially when they have to fight in the fog. If the authorities want to ensure that FIUs (as information processing units) receive quality intelligence they must define the parameters of this intelligence and the precise circumstances that prompt reporting. For the system to work properly the authorities and the respective national FIUs must provide reporting institutions with regular feedback so that the latter can learn how to better assist the FIUs. FIUs also require systematic feedback from the police and prosecutors that would enable them to better focus their efforts. FIUs are obliged to demonstrate that they too are accountable for their missives and their actions; otherwise, like soldiers in the absence of clear commands, reporting institutions may slide back to the old practice of reporting all or nothing, and there is a danger that FIUs will fight the current 'war' on their own with no imminent success.

References

1. Anciberro, S. (2005). *The Third EU AML Directive: Impact on European Banks*. The European Banking Federation, 10 August 2005. http://www.gtnews.com/article/6060.cfm (accessed 28 February 2008).

2. Anderson, A. G. (1979). *The Business of Organised Crime — A Cosa Nostra Family*. Stanford
3. Commission of the European Communities, Commission Staff Working Document. (2006). *The application of Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering in relation to the identification of clients in non-face to face transactions and possible implications for electronic commerce*. SEC(2006) 1792, Brussels, 19.12.2006.
4. Commission of the European Communities. (1998). *Money laundering: how to improve EU rules for prevention*. Special Feature - No 14, October 1998, http://ec.europa.eu/internal_market/smn/smn14/s14mn20.htm (accessed 27 February 2008).
5. van Duyne, P. C. (2003). Money laundering policy. Fears and facts. In P. C. van Duyne, K. von Lampe, & J. L. Newell (Eds.), *Criminal finances and organising crime in Europe*. The Netherlands: Wolf Legal Publishers.
6. van Duyne, P. C. (2004). The creation of a threat image. Media, policy making and organised crime. In P. C. van Duyne, M. Jager, K. von Lampe, & J. L. Newell (Eds.), *Threats and phantoms of organised crime, corruption and terrorism*. Nijmegen: Wolf Legal Publishers.
7. van Duyne, P. C., & Levi, M. (2005). *Drugs and money. Managing the drug trade and crime-money in Europe*. Oxon (UK): Routledge.
8. van Duyne, P. C., Maljevic, A., van Dijck, M., von Lampe, K., & Harvey, J. (2007). *Criminal finances and state of the art. Case for concern?*. Nijmegen: Wolf Legal Publishers.
9. Egmont Group. (2003). *Information Paper on Financial Intelligence Units and the Egmont Group*. September 2003, http://www.egmontgroup.org/info_paper_final_092003.pdf (accessed 13 May 2008).
10. Financial Services Authority. (2008). *Review of firms' implementation of a risk-based approach to anti-money laundering*. March 2008.
11. Freis, J. H. Jr. (2007). *Pan-American congress on asset laundering and financing terrorism prevention and control*. Cartagena De Indias, Colombia, 27 July 2007, http://www.fincen.gov/speech_colombia_072707.html (accessed 28 February 2008).
12. Gilmore, W. (1993). *Money laundering: the international aspect*. Hume Papers on Public Policy, Vol. 1, No.2, Edinburgh University Press, pp. 1–11.
13. Gold., M. & Levi, M. (1994). *Money-laundering in the UK: an appraisal of suspicion-based reporting*. The Police Foundation (London)/University of Wales College of Cardiff.
14. Harvey, J. (2005). Controlling the flow of money or satisfying the regulators. In P. C. van Duyne, K. von Lampe, M. van Dijck, & J. L. Newell (Eds.), *The organised crime economy. Managing crime markets in Europe*. Nijmegen: Wolf Legal Publishers.
15. International Monetary Fund. (2004). *Financial Intelligence Units: An Overview*. http://www.imf.org/external/pubs/ft/FIU/fiu.pdf (accessed 13 May 2008).
16. Joint Money Laundering Steering Group. (2007). *Prevention of money laundering/combating terrorist financing. Guidance for the UK financial sector. Part I and Part II*. December 2007.
17. KPMG. (2007). *Global anti-money laundering survey 2007. How banks are facing up to the challenge*.
18. Lacey, R. (1991). *Little Man: Meyer Lansky and the Gangster Life*. Boston: Little, Brown and Company.
19. von Lampe, K. (1999). *Organised crime: Begriff und Theorie organisierter Kriminalität in den USA*. Germany: Peter Lang, Frankfurt am Main.
20. Levi, M. (1993). *The investigation, prosecution, and trial of serious fraud*. Royal Commission on Criminal Justice Research Study No.14, HMSO, London.
21. Levi, M. (2003). *Controlling the international money trail: a multi-level cross-national public policy review*. Final Report, Swindon, Economic and Social Research Council.
22. McClain, S. K. (2007). *Statement of Deputy General Counsel, Financial Service Centers of America, before the U.S. House Committee on Financial Services, Subcommittee on Oversight and Investigations regarding suspicious activity and currency transaction reports: balancing law enforcement utility and regulatory*. Financial Service Centers of America, Washington, D.C., 10 May 2007, http://www.house.gov.apps/list/financialsvcs_dem/htmcclain051007.pdf (accessed 21 November 2008).
23. Morris-Cotterill, N. (2001). *Think again: money laundering*. Foreign Policy, Carnegie Endowment for International Peace, pp. 16–20. May/June 2001.
24. Pieth, M. (1999). The harmonization of law against economic crime. *European Journal of Law Reform*, 1, N. 4, 527–545.
25. Price, B. (1992). Patterns of drug trafficking and countermeasures: the personal view of a veteran. United Nations Office on Drugs and Crime, 1 January 1992, http://www.unodc.org/unodc/en/data-and-analysis/bulletin/bulletin_1992–01-01_1_page008.html (accessed 31 March 2008).

26. Robinson, J. (1994). *The laundryman: inside the world's third largest business*. Simon & Shuster Ltd.
27. Robinson, J. (2003). *The sink*. London: Constable and Robinson Ltd.
28. Savona, E. (ed.), (1997). *Responding to money laundering international perspectives*. Harwood, Netherlands.
29. Seagrave, S. (1995). *Lords of the Rim*. New York: Putnam.
30. Stessens, G. (2000). *Money laundering: a new international law enforcement model*. Cambridge: Cambridge University Press.
31. Stessens, G. (2001). The FATF 'black list' of non-cooperative countries and territories. *Leiden Journal of International Law*, 14, 199 – 208.
32. Taylor III, A. L. (1984). *Swiss secrets are put to a vote*. Time magazine, 28 May 1984, http://www.time.com/time/magazine/article/0,9171,951110,00.html accessed 10 March 2008.
33. Uribe, R. (2008). *Changing paradigms on money laundering*. The Observer News– second quarter 2003, Inter-American Observatory on Drugs, http://www.cicad.oas.org/oid/NEW/Information/Observer/Observer2_2003/MoneyLaundering.htm; http://www.cicad.oas.org/oid/NEW/Information/Observer/Observer2_2003/MLParadigms.pdf (accessed 24 May 2008).
34. U.S. General Accounting Office (GAO). (1996). *U.S. Efforts to Combat Money Laundering Overseas*. Statement of JayEtta Z. Hecker, Associate Director, International Relations and Trade Issues, GAO Testimony Before the Committee on Banking and Financial Services, House of Representatives, GAO/T-GGD-96-84, http://www.gao.gov/archive/1996/gg96084t.pdf (accessed 29 February 2008).
35. U.S. General Accounting Office (GAO). (1998). *Money Laundering:* FinCEN's *Law Enforcement Support, Regulatory, and International Roles*. Testimony, 04/01/98, GAO/T-GGD-98-83, http://www.fas.org/irp/gao/ggd-98-083.htm (accessed 29 February 2008).
36. Vallance, P. (1992). *Money laundering: the situation in the United Kingdom*. Paper presented to the Council of Europe Money Laundering Conference, Strasbourg, France, 28–30 September 1992 (typescript).