MARK PIETH GEMMA AIOLFI

Anti-Money Laundering:
Levelling the Playing Field

GOVERNANCE
BASEL INSTITUTE ON GOVERNANCE

Foreword

Switzerland is frequently accused of being reluctant to take thorough measures to fight money laundering. Both the Swiss authorities and the banks in Switzerland strongly reject such accusations. We are convinced that our anti-money laundering measures are best market practice.

What are the reasons for these markedly different viewpoints? Can they be explained by conceptual differences? Are the negative statements the result of insufficient knowledge of our legal provisions, or are they simply motivated by the political desire of the respective commentators to divert public attention from the deficient anti-money laundering policies in their own countries? A comparison of our measures with the most important competing financial centres could help to answer these questions. The SFS Stiftung Finanzplatz Schweiz – a foundation initiated by the foreign banks in Switzerland – commissioned Professor Mark Pieth of the Basel Institute on Governance to conduct a comparative study of anti-money laundering regulations in the UK, the US and Singapore, the three financial centres which closely compete with the Swiss private banking sector. Professor Pieth is a renowned expert in the field and has close contacts with the international experts who also contributed to the project with in-depth country studies.

When comparing different legal and regulatory systems we have to bear in mind that each national system consists of at least three layers: firstly, the written laws and regulations; secondly, the implementation of these laws in internal policies, procedures, compliance and audit organisations; and thirdly the corporate culture which guarantees that the regulations actually determine the behaviour of banking staff. Of course, what counts is the sum total of all three layers. The study focuses on the first of these layers, although frequent references are made to the problems of implementation and compliance. The reading of the full text is a rewarding undertaking, not only for the specialist in the field. The Stiftung Finanzplatz Schweiz nevertheless felt that an abridged version – at the same time a summary and the research team's own conclusions on the current state of anti-money laundering regulations – would help make the study's findings known to a wider audience.

Everyone will draw his or her own conclusions from the study. As a Swiss banker I looked for answers to four questions: Where does Switzerland stand? Is our self-assessment correct? How do the other financial centres fare with respect to anti-money laundering policies? Are the negative comments about Switzerland made in public based on facts? My reading of the text answers these questions.

The study explicitly confirms our conviction that Switzerland sets best market practices in customer due diligence and know-your-customer principles. Our self-assessment, then, is therefore justified, even after the legal steps taken by the UK and the US in the aftermath of the September 11, 2001 terrorist attacks narrowed the gap between Switzerland and its main competitors, at least at the formal level. I still claim – on the basis of the facts given in the study – that with respect to compliance and corporate culture Switzerland is still a considerable way ahead. Shop-floor banking reality in the US and the UK has still to catch-up with new legislation. Such adjustments need time, and we hope the gap is just transitional and does not reflect a "benign neglect" attitude on the part of the respective authorities.

Two different concepts of anti-money laundering regulations seem to exist: one based on "retail banking" and the other based on "private banking". The first one prevails in the UK and the US and stresses data gathering and reporting requirements. "Know-your-customer" requirements play a minor role. The standard joke that "KYC" actually stands for "Kill-Your-Career" is symptomatic of the low priority given to customer due diligence and client identification under this concept, at least until very recently. The alternative concept applied in Switzerland and (in principle) in Singapore focuses on strict know-your-customer and due diligence duties. The term "banking secrecy" is a clear misnomer: there is nothing secret between banks and their clients. The

concept is restrictive with respect to data transfer and reporting requirements. Unless the due diligence process shows evidence that money laundering activities are involved, no reports are made. It is no wonder that the number of reports to the authorities differ. But while the "retail -based" concept leads to a large number of reports (although from a very restricted number of banks, as the full study reveals to be the case in the UK) with little evidence of money laundering activities, the "private banking" concept on the other hand delivers fewer reports but with strong evidence and, as a result, a higher probability of a criminal investigation.

It is surprising that the scope of application in the US and the UK is not as broad as it is in Switzerland. In the US, lawyers are not covered by the legislation, and the new requirements to identify the beneficial owner – introduced only recently as a result of the 11 September 2001 terrorist attacks – applies to funds held for non-US persons only. Such a regulation is not only a blunt violation of international standards, but renders anti-money laundering policies ineffective. This regulation reminds us of our own laws discarded more than 20 years ago when a Swiss could act as a "front man" for foreigners without having to disclose the identity of the beneficial owner. One wonders why the two largest financial centres in the world do not put more regulatory emphasis on the areas where they carry out most of their international business. For example, why should the OTC-market be less attractive for money laundering activities than payments made through SWIFT? The UK's Financial Services Authority – the supervisory agency – has even officially announced that priority is to be given to combating money laundering activities in the retail banking system. Such an announcement clearly signals which sectors will not be supervised and monitored with the highest possible scrutiny, and the result will be that "dirty" money will be diverted to services with low levels of supervision.

I am still surprised that in many countries around the world banks are not obliged to identify the beneficial owners of assets. The general impression that Singapore has not made progress in that field is confirmed. The report also draws attention to trusts and other financial vehicles in the UK; one could also add Delaware companies in the US. It is conveniently "forgotten" in public discussion that London is an important centre for offshore transactions which are protected by legislation that does not require the identification of the beneficial owner. Someone once said that the UK and the US do not need banking secrecy as their banks are anyhow not even obliged to know who their customers are.

This brings me to a third aspect which is implicit in the study. Anti-money laundering is formally a legal issue, but it has become a branch of political economy. The study's statement that the UK has pushed for strong international recommendations without developing the same zeal in developing its national law is a striking example. But it is even more striking to see the US pushing for strong Financial Action Task Force (FATF) recommendations, but not implementing them. In 1997 the US was blamed by the FATF for not complying with its recommendations, but it was only after the 11 September 2001 terrorist attacks that the US finally took action.

Why should we worry? All regulation has a public benefit (or should have one) but imposes private costs. The banks which first implement international recommendations carry the regulatory costs first – and alone. The long delay of other competing financial centres or the reluctance of such countries to implement agreed international standards leads to a competitive disadvantage for the complying institutes. Those who win the race of implementing the internationally-agreed standards loose out on the business side.

The international agencies should perhaps give less emphasis to the setting of new standards and more on the monitoring of existing ones. As EU Commissioner Frits Bolkestein remarked (admittedly in a different context): "What is the point of having new legislation if it remains dead in the water?" For once we can agree with him!

Dr. Alfredo Gysi, Präsident SFS Stiftung Finanzplatz Schweiz

Table of Contents

I Introduction

1. The Challenge

Although there is no single definition of money laundering, most descriptions commonly refer to it as the process by which criminals attempt to conceal the source and ownership of the proceeds of their illicit activities. When carried out successfully it enables the criminal to maintain control and access these funds when and where he chooses, and may ultimately provide a legitimate cover for the origin of the income. The efforts to combat this phenomenon are the subject matter of this study, and whilst there is no real disagreement on the need to engage in combating money laundering to counter its divisive social and economic effects, what is striking is the volume and variety of countermeasures; encompassing international and national approaches and crime control in terms of both preventive and regulatory measures. Despite the quantity of rules, there is still a lack of harmonisation and uneven implementation, and even where rigorous systems are in place they may still lag behind the increasingly sophisticated techniques employed by money launderers.

Economic crime is not a new problem, the anti money laundering (AML) paradigm is however a relatively novel concept that has emerged over the past three decades or so. In its original form it was envisaged as a tool that would contribute to the reduction of illicit trafficking in drugs. The concept was subsequently rapidly expanded to cover other predicate offences. From the institutional perspective the focus at the outset was almost exclusively on banks as the obvious 'gate keepers' to the financial systems, and having drawn them into the regulatory system, the focus shifted to non-banking financial institutions (NBFI's) and even non-financial institutions (NFI's). The recent – and ongoing – intensive discussions on obliging lawyers to fulfil reporting requirements, mirrors this development, and has caused concern amongst the profession in the EU as well as in North America.

In parallel to the 'criminalisation' of all offences of obscuring and reintegrating ill-gotten gains and the redevelopment of forfeiture rules the main thrust for the development of the AML paradigm has been in supervisory law: Starting out with the essential rules on the identification of the customer there has been a gradual but continuing shift towards the identification and verification of beneficial owners.

The last decade has seen a concerted drive to secure compliance by all major (and even minor) financial centres of the world to the international recommendations promulgated in this field. In this connection the Financial Action Task Force (FATF), as the organisation spearheading this move, and more recently the IMF have developed monitoring mechanisms for their members and even non-members. This latter group have been pressured to commit to formal compliance at least, with a 'robust' policy of using the threat of blacklisting of non co-operative countries and territories (NCCT).

At the present time we are however, witnessing a major reformulation of AML with far-reaching implications both for the authorities tasked with implementing the rules and more especially for the private sector. This reformulation can be summarised as the shift from a 'rule based' to a 'risk based' approach in the implementation of the AML rules. It may be that this change is to some extent just a reshuffling of ideas and approaches that were already in place before – nevertheless the impact on financial institutions world-wide cannot be underestimated. Banks and other financial services providers find themselves obliged to take responsibility for screening their clients according to certain risk factors. Financial institutions are being increasingly drawn into doing what so far had been the task of the public sector: anticipating risk, defining the details, for example in relation to what constitutes terrorist threats, defining profiles for what are termed politically exposed persons (PEPs) etc.

The consequence of being responsible for formulating these criteria has been the toughening up of reporting requirements and the contradictions of this approach were particularly highlighted in the aftermath of September 11th. In order for financial institutions to be able to take advantage of the flexibility of managing risk they still need clear, abstract rules to inform their approach.

As AML develops it is quite justified to ask how effective are all these measures. However the answer is hardly to be found in conviction statistics or the amount of assets confiscated. The reason being that not only has the scope of predicate offences expanded steadily making the interpretation of data problematic, but also the very nature of the traditional core element of drug money laundering means that effectiveness cannot be measured with any real accuracy. What can be measured is the level of suspicious transaction reporting, and in places where there is a so called 'early warning system' (such as the UK) there are comparatively large numbers of notifications (e.g. in the UK over 30,000 in 2001), but when criminal investigation statistics or the conviction rate is looked at there these numbers dwindle dramatically to a mere handful. The pattern is not dissimilar when it comes to the confiscation of assets, with some countries changing their laws in order to try to increase their success rate. Thus effectiveness in terms of convictions and confiscation is but one aspect, and altogether not a very satisfactory indicator. On quite a different level, the development of AML regulations has been about creating internationally compatible instruments of information about capital movements, with the aim of tracking global money flows to control risk, and here the background has been the creation of a level playing field for financial institutions. Therefore effectiveness is also about comparing the implementation of international standards with a view to minimising regulatory arbitrage – hence the increasing focus on offshore centres (OFCs) and certain corporate vehicles.

So the question now is, is the 'playing field' being levelled in AML? This question cannot be settled with a one word answer: the vigour with which a country tackles the problem of money laundering, may have repercussions for its competitiveness as a financial centre. This in turn results in a politicisation of the topic – in particular in relation to setting the parameters to defining the activities that fall within the scope of criminal behaviour. Thus this fundamental debate as to what constitutes criminal behaviour in AML terms has also spilled over into the international arena, where some countries consider that this issue will continue to vex the question as to whether the field can ever be regarded as level.

2. Impact on major financial centres

The aim of this study is to describe in general terms the modifications to which AML has been subjected (in sections II and III below), and then to analyse how AML impacts on four of the major cross-border banking centres (namely; UK, USA, Singapore and Switzerland). Thereby the study will highlight in a brief manner, the transition of AML concepts pre- and post 2000 within these major financial centres (section IV). This summary is the shortened version of an extended study conducted in 2002-2003[1].

1 Study by the Basel Institute on Governance commissioned by the Stiftung Finanzplatz Schweiz, Towards a Level Playing Field in Cross Border Banking: Comparing Anti-Money Laundering Rules (UK, USA, Singapore, Switzerland), December 2002.

II Developing the standards

1. Creating a new paradigm

Being a relatively new concept the question then arises why did the concept of AML emerge when it did, towards the end of the 20th Century? The response commonly put forward refers to the accumulation of capital from illegal markets, more specifically the burgeoning drugs trade which was regarded as having the potential to destabilise economies, which could in turn pose threats to public order. At the same time the 1980s witnessed the twin developments of deregulation and globalisation of both markets and industries, facilitated by technological developments. Criminals seeking to launder the proceeds of crime were able to benefit from these advances, and whilst law enforcement efforts were largely constrained by territorial concepts, money launderers were not.

In America the pressure to deal with the problems caused by the drugs trade came to a head with the declaration of the 'war on drugs'. This policy entailed going for the money with the aim of cutting off the cash supply that feeds the trade at every stage. In order for this to be effective at all it was quickly recognised that the approach would not only have to oblige financial institutions to maintain a 'paper trail' with respect to cash transactions but also for the approach to be comprehensive, world-wide implementation would be needed. Therefore the choice of the UN as the body for the next stage of the development of AML was entirely logical. In 1988 the *UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* saw the light of day. This treaty introduced the criminal law aspect of money laundering and established the agenda: forfeiture of ill-gotten gains, criminalisation of money launderers (be it individuals or companies), mutual legal assistance and extradition.
However, the subject did not rest with the UN, not least because the USA, UK and France took the view that this route would not necessarily safeguard financial institutions against money laundering of drug proceeds. Acting within the G7 context these countries were instrumental in establishing the FATF.

2. The origins of customer due diligence

The emergence of customer due diligence (CDD) was an entirely separate though parallel development. The origins of CDD rules are to be found in prudential law and internal risk management within financial institutions, founded on traditional good practice that starts from the premise that by understanding the customer's business and conducting diligence checks that this is the most effective way of minimising exposure for instance to the effects of accumulated risk. And it was the Swiss experience in this area that turned out to be an important contribution to the development of CDD. The Chiasso banking scandal in the 1970s prompted the Swiss National Bank together with the Swiss Banker's Association to draft the first version of the Swiss Bankers Code of Conduct (CDB) in 1977, this gentlemen's agreement between the banks and the Swiss Banker's Association set out guidance on customer identification, addressed issues of active support of tax evasion, the treatment of domiciliary companies, and developed the notion of beneficial ownership in KYC. Whilst the motivation at that time was the safeguarding of its reputation as a financial centre, the Swiss CDB influenced subsequent international texts such as the Basel Statement of Principles (BSP) and even sections of the Forty Recommendations of the FATF.

Concerns that public confidence in the banking system could be undermined through the latter's association with

criminals, led the Cooke Committee of the Bank for International Settlements to adopt the BSP in 1988. This set of recommendations broke new ground in that bank supervisors agreed for the first time on the risks associated with the abuse of the financial system where '*money derived from criminal activity*' is involved. The BSP text addressed the issue of 'know your customer' in terms general presaging the merging of CDD into the AML system, to be taken up again in the FATF Forty Recommendations where both criminal law standards and regulatory aspects are drawn together.

3. Merging standards and broadening their scope

Despite the fact that the UN had just adopted its 1988 anti-drug Convention [2] and the BSP had been written, the G7 countries – and the USA, UK and France in particular – were not satisfied that these measures would be sufficient to prevent the use of financial institutions for the laundering of drug proceeds. In 1988 at the G7 meeting in Harrisburgh, USA, the Americans proposed the creation of a task force to promote the programme of the Vienna Convention, this was opposed at the time by France but then reinstated by them a year later at the G7 Paris Summit in 1989, on condition that they had the initial chairmanship and that tax offences be included in the FATF's remit. Switzerland, Luxembourg and Austria agreed to support the effort only if tax issues were taken off the agenda. Once the compromise was settled, the FATF was initially established as an ad-hoc body but which has continued to be a major agenda-setter in preventing money laundering.

Although AML started out as a means to deal with the proceeds of drugs, the range of predicate offences was fairly quickly extended to all serious crime, making it available as a tool to be used in the fight against graft, to assist in the repatriation of assets and in some jurisdictions into a 'blanket concept' to be tagged onto all sorts of crime. This breakthrough in the extension process came about in 1996 within the FATF, which adopted the reference to 'serious offences', whilst leaving it to individual countries to designate which offences should be regarded as 'serious'.

In the same vein, there has been a steady attempt to close all the entry points into the financial system. Having started with the obvious gatekeepers – the banking sector – the focus then shifted to NBFIs and then to NFIs. The focal point for the most recent discourse has centred on how to include lawyers in the AML system, and specifically whether they should also be obliged to report suspicious transactions to the authorities, raising concerns about legal professional privilege. This debate has been conducted within the EU as well as in Australia, New Zealand and currently Canada. It is an issue that is also picked up in the FATF Consultation Paper published in 2002 and which provoked strong comments from lawyers groups around the world.

Having extended the institutions subject to AML, reporting requirements were also gradually toughened up. In 1996 the FATF made reporting obligatory although Member States can choose whether to create a specialised *Financial Intelligence Unit (FIU)* or to define reports as complaints to law enforcement bodies. In some countries *Suspicious Transaction Reports (STRs)* were sent directly to prosecution authorities but a criminal investigation would not necessarily result because the requisite qualified suspicion was lacking. Additionally law enforcement

2 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances adopted in Vienna on 19 December 1988 ('Vienna Convention').

authorities are typically organised locally and would not have the capacity to liase systematically with foreign counterparts[3].

On the other hand, a theoretically and practically significant development was triggered off by the reformulation of reporting requirements in 1996. Some countries have extended the notion of 'suspicion', for instance, the Netherlands explicitly request *'unusual circumstances'* to be notified to authorities, the UK and the US have similarly early notification systems albeit using more implicit language. This arrangement has serious consequences for the number of notifications filed[4]. Other countries insist on actual suspicion, thereby keeping the number of notifications rather low (France, Germany and Switzerland[5]). Of course there is also a direct correlation to the quantity of notifications processed into criminal investigations – an unusual transaction notification system would generate probably less than 5 % criminal investigations, whereas the corresponding figure for a suspicion-based system could be well over 50 %[6]. Therefore a corresponding degree of caution has to be exercised when comparing statistics from these countries.

4. 'Spreading the gospel' and securing compliance world-wide

Various organisations and supra-national bodies ranging through the FATF, EU, CoE, OAS, and the IMF have achieved a remarkable success in changing the international legal and regulatory landscape, in their different ways. The FATF though, was the body that first developed a monitoring mechanism.

The monitoring mechanisms of the FATF have been described as a *"major departure from the traditional view that implementation of treaties and conventions was a purely domestic matter"*[7]. Whereas the *"Self Evaluation Procedure" (SEP)* allows members to describe their approach in their own words in a procedure followed annually on the basis of a standard questionnaire, the *"Mutual Evaluation Procedure" (MEP)* relies on the on-site visit of experts from Member States to conduct interviews and give their critical judgement to the Group. In the course of intensive negotiations with the Group an evaluative text is finalised[8].

The teeth to this monitoring mechanism are the threat of sanctions for failure to comply with the FATF Recommendations. These threats have been used to prompt members into action, although a somewhat different stance was taken towards non-FATF member states. This manifested itself by the FATF membership taking the view that the ability of its members to protect themselves against money laundering could be undermined if non-member jurisdictions did not adopt and implement the Recommendations as well. In what was an unprecedented move, the FATF chose to go beyond its original mandate to assess its own members[9], and in 1998 it initiated the process to identify *Non-Cooperative Territories and Countries (NCCTs)*, thereby going beyond the peer evaluation process. The FATF thereby joined a general trend pioneered by other organisations to develop the discourse on money laundering and related issues beyond the traditional link to predicate offences and re-conceptualise it as a problem of under-regulated OFC's. In its initial report on NCCTs published in 2000,

3 Cf. Germany and Critical Comments, PIETH 1998, p. 159 et seq.
4 Cf. KILCHLING 2002, p. 431 et seq.
5 Ibid.
6 Switzerland: over 70 % in 2000, up to 80 – 90 % in 2001. (cf. MROS, 3. Rechenschaftsbericht für das Jahr 2000, p. 10 and 4. Jahresbericht für das Jahr 2001, p. 9)
7 LEVI/ GILMORE 2002, p. 94.
8 SANSONETTI 2000, p. 218-226; www.fatf-gafi.org.
9 WINER 2002, p. 30.

25 criteria consistent with the Forty Recommendations were defined[10]. The process described was to identify jurisdictions clearly falling below the established world-wide standard and to encourage them to enact and apply the necessary laws. In June 2000, without making approaches to the potential candidates through diplomatic channels (as had been done with the deficient Member States), the FATF went straight into publishing a first review in which 15 jurisdictions were identified as NCCTs on its famous black list[11].

On the one hand the process had left the crucial question open as to what the consequences of blacklisting would be. On the other, a process has already set-in within the banking industry to apply increased diligence to NCCTs. This has been a strong motivating factor for countries like Liechtenstein to amend their legislation in a very short period of time[12] and to rush identification not only of new but also of existing client relations[13] in order to be delisted[14].

5. Redefining the problem

A closer examination of the materials reveals that from the outset AML initiatives were not exclusively directed at combating criminal behaviour. Historical evidence shows that the US administration in particular, attempted, from the first negotiation round within the FATF in 1989 to raise the Central Bank's ability to produce meaningful aggregate data on financial flows (in cash and electronically)[15]. As a consequence of the liberalisation of financial markets and the increasing pace of globalisation national control over financial markets was regarded as being in danger of losing its grip. As the FATF was not necessarily the right institution to promote macroeconomic policy instruments the issue was picked up by the IMF in its 1996 and 1997 *'Data Dissemination Standards'*[16] and its *'Code of Good Practices on Transparency in Monetary and Financial Policies'* of July 1999.

Whilst concerns about the stability of financial markets in macroeconomic terms may have been a hidden subtext to the FATF discourse from the early days, this issue has been put on the international agenda in a much more prominent way by the creation of the *Financial Stability Forum (FSF)* in February 1999. This G7-initiated body was created to *'promote international financial stability, to improve the*

10 FATF Criteria for Defining Non Co-operative Countries or Territories (14 February 2000), available at http://www1.oecd.org/fatf/pdf/NCCT_en.pdf, cf. also FATF XI, Report p. 18 et seq.

11 FATF Criteria for Defining Non-Cooperative Countries or Territories (14 February 2000).

12 Gesetz vom 22. Mai 1996 über die beruflichen Sorgfaltspflichten bei der Entgegennahme von Vermögenswerten (revised version enacted as of 1 January 2001).

13 Letter of Commitment des liechtensteinischen Bankenverbandes 17 July 2000; Pressemitteilung des liechtensteinischen Bankenverbandes über die Ausdehnung der Sorgfaltspflicht 19 July 2000.

14 A goal achieved in 2001.

15 US Working Group documents, WG I & II FATF I 1989/90; See also PIETH 1998, p. 161; idem. 1998/9, p. 532.

16 IMF, Special Data Dissemination Standard (SDDS), March 1996; General Data Dissemination System (GDDS), December 1997; (cf. http://dsbb.imf.org/gddsweb/whatgdds.htm).

functioning of markets, and to reduce systemic risks through enhanced information exchange and international co-operation in financial market supervision and surveillance'[17]. On 25 May 2000, the FSF published a list of *'jurisdictions considered to have significant financial off-shore activities'*[18]. The list distinguishes between three categories of jurisdictions, reflecting their perceived quality of supervision and degree of co-operation.

Shifting from the narrow focus of 'money laundering' to 'control of OFCs' implied that a definition of OFCs was required: Earlier neutral definitions of off-shore banking referring to banking abroad, meaning outside the domestic territory of commercial activity, were superseded and the notion of off-shore centre rapidly became morally tainted and the expression was used as an equivalent to a 'regulatory' or 'tax haven'[19]. When referring to off-shore financial centres reference was typically made to the services they offered, specifically the rapid and cheap incorporation of domiciliary companies *('International Business Corporations' [IBCs])*, a minimal regulatory and supervisory structure and a combination of strong customer confidentiality laws with inadequate mutual legal assistance[20].

An integral part of the drive to control OFCs is the work on **corporate vehicles** used to obscure the provenance of funds. Within the FATF such efforts started in 1993 with the discussion on *'shell corporations'*[21], it was continued over all these years but brought to more prominence in the OECD report *'Behind the Corporate Veil'*[22]. The topic of trusts and corporate entities is a subset of a wider issue, namely the identification of the beneficial owner, and new drives to make progress on CDD were initiated by the Basel Committee on Banking Supervision culminating in the publication of its *'Customer Due Diligence for Banks'* in October 2001.

17 FSF, International Standards and Codes to Strengthen Financial Systems, April 2001, p. 19 (http://www.fsforum.org/Standards/Repiscsfs.pdf+International+Standards+and+codes+to+Strengthen+financial+systems&hl=de&ie=UTF-8); Cf. also SANSONETTI 2001, p. 40.

18 Financial Stability Forum Releases Grouping of Offshore Financial Centres (OFCs) to Assist in Setting Priorities for Assessment (http://www.fsforum.org/Press/P20000525.html; http://www.bis.org/press/p000526.htm).

19 UN ODCCP, Paradis financiers, sécret bancaire et blanchiment et d'argent, Vienne, 19 Mai 1998.

20 "International Co-operation in the Fight against Corruption and Off-shore Financial Centres: Obstacles and Solutions", Conference of the Council of Europe, Limassol, 20 – 22 October 1998; Inter-governmental Expert Group of the UN for the Prevention of Crime and Criminal Justice, Meeting in Paris 30 March – 1 April 1999: "The Corruption and the International Financial Circuits: Elements of a Global Strategy in the Fight against Corruption"; a similar definition is used by the OECD Working Group on Bribery, cf. DAFFE/IME/BR/WD 2000(4), 16 February 2000, p. 6.

21 Shell Corporation Typology, US Department of Justice (DoJ), 1993.

22 OECD "Behind the Corporate Veil – Using Corporate Entities for Illicit Purposes", Paris 2001; cf. also the private study by WYMEERSCH 2001; SAVONA 2002.

III Sharpening the focus of CDD: From a 'rule based' to a 'risk based approach'

1. The 'Revolution'

When the FATF defined CDD for its purposes of combating money laundering in 1989/90 it used a model based on five obligations of financial operators:

- They were obliged to *'identify the immediate client'* (regular clients under all circumstances, occasional clients above a threshold) and verify their identity based on official documentation. Additionally, they were to identify *'beneficial owners'* if they clearly differed from the immediate client (here the text was silent on verification)[23];
- They were to apply increased diligence when confronted with *'complex, unusual large transactions'* or *'unusual patterns of transactions which have no apparent economic or visible lawful purpose'*[24];
- They were to record information (sub indent 1 and 2), and to maintain records for at least 5 years[25];
- They were to report suspicion of money laundering to the competent authorities (FIUs)[26];
- They were to develop in-house compliance concepts, train their employees, and introduce an audit function to test the systems[27].

The **more recent** documents on CDD apply a somewhat different methodology, influenced by the practical needs of the industry (meaning primarily cost considerations): First the concepts distinguish between obligations in the **client-acceptance** procedure[28] and **ongoing monitoring**[29].

Under the heading of **KYC** they go **beyond** the original **formal identification** requirements for natural and legal persons. Within KYC the current standards request financial entities to seek enough information from their clients to understand the client's business[30] in order to detect unusual transactions or patterns of transactions[31]. Whereas the original formulation of 1990 had left it to the intuition of the account manager whether he or she detected transactions out of tune with the information they had of their client[32], the more recent standard requests the collection of substantive information on the client, in the context of private banking they go as far as requesting a 'client profile'[33]. Additionally, if corporate vehicles or trusts are involved, the financial operator is requested to understand the '*structure of the company sufficiently to determine the provider of funds... and those who have control over the funds*'[34]. KYC has developed from a formal routine documenting of identity to a complex process of understanding the client's business. However, immediately the question crops up how much time, effort and ultimately money needs to be invested into CDD. The answer is not an absolute one, rather the current discourse on CDD offers a new approach.

In the early days when supervision moved into the area of preventing money laundering in order to safeguard public trust in the banking industry, supervisors defined the risks and the measures to be taken by banks. Financial operators would follow specific rules. Banks risked sanctions for non-compliance, on the other hand, their responsibility was qualified if they followed the rules. In many instances the rules proved to be unnecessarily burdensome and procedures invited purely formal compliance. In other situations they were inadequate because they did not necessarily take specific increased risks into account.

The situation was addressed by an alternative approach, which has developed out of the established practice of self-regulation in some countries: The **risk-based approach** shifted part of the

23 FATF 40/1990, Rec. 12, 13; FATF 40/1996, Rec. 10, 11.
24 FATF 40/1990, Rec. 15; FATF 40/1996, Rec. 14.
25 FATF 40/1990, Rec. 14; FATF 40/1996, Rec. 12.
26 FATF 40/1990, Rec. 16–19; FATF 40/1996, Rec. 15–18.
27 FATF 40/1990, Rec. 20; FATF 40/1996, Rec. 19.
28 BCBS CDD 2001, § 20; FATF Cons. Paper 2002, § 29 et seq.; WB, Art. 1 and 2.
29 BCBS CDD 2001, § 53 et seq.; FATF Cons. Paper 2002, § 29 et seq.; WB, Art. 3 and 5.
30 BCBS CDD 2001, § 26 et seq.; FATF Cons. Paper 2002, § 29 et seq.; WB, Art. 1.2.2.
31 BCBS CDD 2001, § 53 et seq.; FATF Cons. Paper 2002, § 29 et seq.; WB, Art. 1 and 4.
32 see FATF 40/1990, Rec. 15; FATF 40/1996, Rec. 14.
33 BCBS CDD 2001, § 21 et seq.; FATF Cons. Paper 2002, § 29 et seq.; WB, Art. 1 and 2.
34 WB, Art. 1.2.2.

responsibility for defining the risks, for developing countermeasures and, above all, for a dynamic risk management onto the institution. This approach had the advantage of allowing banks a relatively **simple** and cheap **ordinary procedure** for retail banking and cases without specific risk factors in general. However, as soon as risk indicators became apparent, they were expected to react with a finely calibrated concept[35] of asking intelligent questions, of building a body of information on the client, on matching information on his regular activities with transactions[36]. They were to ask questions about the source of the wealth, possibly the destination, the economic reason for the transaction and, if it did not appear to make sense, additional explanation, up to the point where the professional financier was satisfied or where clarifications left him uncertain, possibly even suspicious of his client's activities.

Of course, also this latter form of regulation although being result oriented, is 'normative' in the sense that financial institutions develop 'compliance rules' to be followed by their officials. It is decisive, however, that the institution carries a large part of the responsibility. And at the same time the institution is granted a margin of discretion.

If the banking and indeed, the wider financial community has to put up with an increasing density of regulation, it has – as a kind of counterweight – managed to convince supervisors of the benefits of a risk-based approach for both sides. This is probably the most decisive impact of the Wolfsberg Group and its discourse with regulators.

The BCBS also introduces its paper by sketching the risk-situations, it anticipates different standards according to the kind of banking[37] and the risk intensity of the type of customer[38].

The generally used format in all new documents distinguishing between client acceptance procedures and ongoing monitoring[39] reflects the experience that it is often the case that risk indicators emerge only over time and depend on building a profile of the client with the obligations under the ongoing monitoring procedures the same as those under the account opening procedures. Additionally, banks will define the role of compliance units, checking on account managers, as well as the use of automated systems to select cases for closer checking[40] .

Both on customer identification and the identification of **beneficial owners**[41] the emphasis of the new standards has shifted from documentation to **verification**[42]. This may lead to a significant increase of work in banking practice.

Especially understanding the control structure and determining the beneficiaries of the **corporate entities and trusts** will require far greater attention[43]. Whereas all the texts accept that there are legitimate uses for complex corporate structures and trusts, they insist on means to prevent the use of a "front" for others[44]. Here the Wolfsberg text is relatively short. Its main emphasis is on understanding the structure of the legal entity[45]. The BCBS's standards go further, especially when discussing special care in cases of companies with **nominee shareholders** and **bearer shares**[46]. Some of the ideas put forward, specifically those regarding bearer shares, originate from the OECD's 2001 report *'Behind the Corporate Veil'* [47] and are picked up in great detail by the FATF Consultation Paper[48].

35 The BCBS CDD 2001 talks of 'graduated customer acceptance policies' (§ 20) and of the need to be 'risk-sensitive' (§ 53).
36 Cf. e.g. Wolfsberg Principles, Art. 1.3 at www.Wolfsberg-Principles.com.
37 BCBS CDD 2001, § 20.
38 Ibid.
39 BCBS CDD 2001; FATF Cons. Paper 2002; Wolfsberg Principles.
40 Cf. WB, Art. 5.1.
41 BCBS CDD 2001, § 21 et seq.; FATF Cons. Paper 2002, § 29 et seq.; WB, Art. 1.2.2.
42 BCBS CDD 2001, § 23, 32 et seq.; FATF Cons. Paper 2002, § 29 et seq.; WB, Art. 1.
43 BCBS CDD 2001, § 32-34; FATF Cons. Paper 2002, § 172 et seq.; WB, Art. 1.2.2.
44 BCBS CDD 2001, § 32.
45 WB, Art. 1.2.2.
46 BCBS CDD 2001, § 33, 34.
47 OECD "Behind the Corporate Veil – Using Corporate Entities for Illicit Purposes", Paris 2001.
48 FATF Cons. Paper 2002, § 196–211.

2. Involvement of the private sector in developing rules and development of the paradigm

In looking at the diverse status of texts like the BCBS, the Wolfsberg Principles and the FATF Recommendations, it would be inappropriate to place intergovernmental texts and private 'gentlemen's agreements' on an equal footing. Nevertheless, the current development is more driven by the discourse between these organisations than it may at first seem.

Although the first edition of the Wolfsberg Principles did not introduce new concepts going beyond the standards of traditionally well-supervised countries, Wolfsberg has participated both in the consultations with the BCBS and the FATF and has adapted its 2000 version in a first review in 2002 to these texts[49]. On the other hand, the BCBS and representatives of the FATF have participated several times in seminars organised by the Wolfsberg Group and have exchanged views. Finally, the OECD Working Group on Bribery has invited representatives of all these organisations to participate in its discourse on OFCs and the prevention of corruption-related money laundering.

With their acceptance and adoption of a risk-based approach as a method to deal with AML, the inter-governmental organisations have recognised the crucial contribution of self-regulation of the financial industry and how to harness it efficiently[50]. This approach relies on financial institutions taking a share in the responsibility of rule making and actively engaging in risk management[51], this **'empowerment'** of the private sector enables it to take a hand in influencing and developing the agenda. At the same time the system is also favoured by the state, because it not only passes the costs of implementation to industry but also extends the reach of criminal law. This explains to some extent why the further development of due diligence is currently pushed forward in a configuration that involves inter-governmental organisations/government agencies, members of the private sector and civil society.

3. Difficulties and contradictions

Unusual transaction reporting which is a feature of the so called early reporting systems allows financial institutions to shift responsibility for outcomes from themselves to the authorities, who then tell the financial institutions how to manage the client relations in question[52]. On the other hand, the overall tendency of AML concepts is moving away from a 'rule-based' towards a 'risk-based' approach to CDD. This latter approach implies the sharing of the responsibilities between supervisors and members of the industry, possibly mediated by groupings of the industry, or more formally structured co-operation bodies sometimes even endowed with regulatory powers[53]. The management of risk utilises the professional know-how, experience and also the differentiated approach of financial institutions to understand the economic background of financial transactions and the often complex financial structures on which they are predicated. There is – at a minimum – an open issue here, if not indeed a risk of contradiction in the approaches put forward. If financial institutions are to

49 WB AML-principles, revised edition, May 2002.

50 PIETH 2002 (Festschrift für Lüderssen), p. 317 et seq.

51 Cf. FATF 40/1996, Rec. 19; BCBS CDD 2001, § 55–59.

52 Cf. suggestions made by the FATF in its Cons. Paper 2002, § 127 et seq.

53 UK: Financial Services and Markets Act 2000. Switzerland: Swiss Banking Commission Regulation 91/98 referring to the CDB.

take responsibility they need clear abstract rules and guidance, but they also need leeway for concrete risk management. Clarification of this discrepancy will come about through deliberations between the 'triangle' of the FATF, BCBS and, for instance, the Wolfsberg-Group.

It has typically been the domain of regulators to **define relevant risks**[54], and this means that beyond financial risks a broad array of operational risks are now to be controlled. Amongst them particularly prominent are legal (which are almost always also reputational) risks. They call to attention money laundering following serious crime, especially drug trafficking, then risk of abuse by PEP's and lastly, financing of terrorism.

Typically regulators request financial institutions to **categorise** their clients according to the risks they pose and the type of services they request. They ask institutions to define the necessary **measures** to be taken for each category and to **collect** the **information** from their clients to determine whether their activities diverge from a pre-defined **customer profile**.

Some regulators have gone as far as to indicate **risk factors** to be considered when defining risk categories[55]. The lists typically comprise:

- **geographic** factors
- for **natural persons** place of origin, place of business activities (and the possible exposure of such places to intensive corruption and money laundering)
- for **legal persons** the place of incorporation (OFC-awareness)
- **personal** factors: PEP's
- **business** related factors: particularly exposed sectors like the defence industry etc.
- **product** related factors: the traditional "red flag list" published regularly since 1990 by regulators (i.e. back-to-back loans)

The industry's responsibilities dove-tail into the regulatory standards. For the industry the 'risk-based approach' has definite advantages. Even if it requires a high degree of attention and corresponding investments, it allows the firms to differentiate radically between low-risk client segments, in which it will be sufficient to go through formal identification procedures and higher risk segments where they would concentrate their diligence efforts. Nevertheless, more and more firms are introducing computerised filter-systems to identify higher risk clients and to monitor ongoing client behaviour against their own behavioural pattern in the past. Atypical transactions or requests would raise alerts and would require personal attention by trained compliance personnel. Closer attention will be given to specific high risk segments. This does not mean that PEP's for example, are to be viewed as a risk category *per se*, but it will result in increased scrutiny of the source of their wealth. On a routine basis a higher standard is required in private banking with high-net worth clients.

The main difficulty in the construction of these risk categories and their implementation in automatic filter systems remains the vagueness of the overall criteria: what is a high risk country? To mention only one example. The official AML bodies, be they international organisations or regulators, will refrain from giving this type of operational advice since they are not only hidebound by political constraints, but it would also contradict the concept itself, where decisions are delegated to the industry. To date, the FATF considers any of its member countries as belonging to the 'regulated world', even though it is evident that risk wise there will be substantial differences.

54 Cf. BCBS 2001.

55 Cf. AML Ordinance issued by the Swiss Banking Commission.

IV The impact of changes in AML on the major cross-border banking centres

1. Introduction

Are the major financial centres and are the competitors in the industry living up to the standards defined internationally? Instead of measuring the impact on organised- and other forms of crime, the public discussion on AML is about compliance with legal and regulatory requirements. Within companies it is about preventing reputational risk. At the political level it is about securing a level playing field for the financial industry and impeding regulatory arbitrage amongst financial centres[56]. It would not be difficult to show that the international peer-review mechanisms, especially the procedures developed by the FATF for members and for non-members are restricting themselves to measuring **formal** compliance. As a consequence, "effectiveness" has been reformulated in relative terms of 'customer due diligence' and comparable standards of risk management.

In looking at the question of the level of implementation of the international standards in the major financial centres in the UK, USA, Singapore and Switzerland, a broad, two pronged approach was taken: Each country was reviewed 'vertically' to ascertain the effectiveness of its AML concept within the country itself, these reviews were then examined 'horizontally' to obtain a comparative overview.

2. Singapore: 'Using the right words'

Singapore has evolved as a financial centre as a result of dedicated policies and legislation specifically aimed at creating a leading financial centre within a short time, which have included deregulatory policies designed to increase competitiveness. The thriving financial centre that Singapore has become is attributable in part to the economically active Chinese minorities in Malaysia and Indonesia who have been looking for a safe harbour for their earnings. Singapore has been acutely aware of the ethnic and political sensitivity of their position, and the delicate relationship Singapore has with its neighbouring countries has also had its impact on the way it has evolved as a financial centre and has defined its AML concept. As long as Singapore was catering for the local market it drew little attention to itself, however, having developed ambitions to become an international player focusing on the SE Asian market, its serious regulatory deficiencies were revealed, drawing harsh criticism from the FATF. This then prompted legislative changes, the effectiveness of which are still uncertain.

The relevant government body for AML matters is the **Monetary Authority of Singapore** (MAS), chaired by the Minister of Finance, the Central Bank, somewhat atypically, has become the main regulating body for the financial services industry and it regulates a wide range of institutions with a firm hand.

Considering that conditions of corruption and questionable public governance prevail in the region, it may not be a coincidence that until 1999 the AML concept in Singapore was narrowly focused on drug-money laundering and there was no formal obligation to notify suspicious transactions. Informal mechanisms to mediate between conflicting interests have not, however, prevented Singapore from being heavily **criticised** by the FATF in its 1999 review.

In an effort to change the situation swiftly, Singapore has conducted a complete overhaul of its AML-system: Three new legal texts **upgraded** the **criminalisation** of money laundering and the ability to confiscate ill-gotten gains (the Corruption, Drug Trafficking and Serious Offences Act [CDSA 1999]), the **regulatory** approach to money laundering (six sectoral MAS Guidelines on Prevention of Money Laundering of 22 February 2000) and the ability to accord **mutual legal assistance** (Mutual Legal Assistance in Criminal Matters Act [MACMA 2000]). Since these legislative and regulatory changes are quite recent, it is difficult to assess their impact as yet.

56 UK: Group of Six Banks Statement on Accounts predating the 1993 Regulations.

The rules criminalizing money laundering were originally contained in the Drug Trafficking Act (DTA) 1993. In 1999 they were amended to extend the list of predicate offences (currently 182 additional non-drug related serious offences). The list of predicate offences does not, however, contain fiscal crime. The construction of the offences largely followed UK law, creating five basic offences: (i) assisting in the retention of the benefits of crime[57]; (ii) concealing or transferring[58]; (iii), acquiring proceeds[59]; (iv), failure to disclose knowledge or suspicion[60]; and (v), the offence of "tipping off"[61]. Unlike the UK, the prosecution does not have to prove that the defendant had actual knowledge that the proceeds derived from crime. An objective knowledge standard lets "reasonable grounds to believe" suffice. A body corporate is deemed to be liable under the CDSA for the conduct of its employees or agents acting within the scope of their actual or apparent authority.

The public prosecutor can apply for a confiscation order against a defendant who is convicted of drug trafficking or another serious offence with respect to benefits of the offence if the court is satisfied that they are thus derived. There is a rebuttable **presumption** that the defendant derived benefits from the offence if they appear disproportionate to his own sources of income and cannot be explained to the satisfaction of the court[62]. The approach to confiscation chosen by Singapore does not insist on the confiscation of the physical assets tainted by the crime, it adopts a **value confiscation** on the basis of an assessment by the court backed up with default sanctions, including long-term imprisonment.

True to the common law tradition provisory, **seizure and freezing** of assets has to be ordered by a judge. For restraint and charging orders the court needs to be satisfied that there is reasonable cause to believe that benefits have been derived from a predicate offence by the defendant.

Mutual legal assistance remains one of the weaknesses of the Singaporean AML system: Even under the new law (MACMA 2000), enacted after criticism from the FATF, coercive measures require a treaty base. MACMA provides the framework within which mutual legal assistance treaties will be negotiated. So far, however, only one such treaty has been concluded (with the US, although negotiations have been initiated with other countries).

Singapore's **bank secrecy** law in a "general rule" states that *"customer identification shall not, in any way, be disclosed by a bank in Singapore or any of its officers to any other persons except as explicitly provided in the banking act"*. This confidentiality applies to customer identification which means any information relating to an account of the customer of the bank, including deposit information. Furthermore, Singapore is one of the only financial centres in which "numbered accounts" can still afford anonymity to the client.

However, there have been some amendments to the bank secrecy law in 2001, so that it may be relaxed in certain situations. Unfortunately though, some uncertainties still remain. For example, it appears that a bank can disclose customer information in relation to a specified list of laws. It seems rather curious that the serious crimes act is not on this list. On the other hand the serious crimes law provides the party disclosing information with protection to the extent that the disclosure will not be a breach of any obligation of confidentiality imposed either by law, contract or rules of professional conduct.

The MAS Notices together with the Association of Bankers' Guidelines 2001 contain detailed and comprehensive rules on **CDD**. Failure to abide by the MAS rules could result in the loss of

57 Sections 43(1) and 44(1) of the CSDA.
58 Sections 46(1) and 47(1) of the CSDA.
59 Sections 46(3) and 47(3) of the CSDA.
60 Section 39(1) of the CSDA.
61 Sections 48(1) and (2) of the CSDA.
62 Sections 4 (2)(5)(6) and 5(2)(5)(6) of the CSDA.

the operating licence. In its self-evaluation to the FATF for 2001/02 Singapore admitted that it was only in partial compliance with Recommendation 19 of the FATF, detailing the NBFI's to be included[63]. Deficits in the coverage of intermediaries, such as fiduciaries and lawyers remain. Referring to the FATF Forty Recommendations and the Basel Committee Statement of Principles of 1988, the MAS Guidelines oblige banks to implement comprehensive compliance programmes.

The KYC rules include special rules for the identification of corporate vehicles and trusts. As to the identification of **beneficial owners**, the relevant MAS Notice does mention the issue in relation to ongoing relationships, not however, when detailing the obligations for the opening of accounts. If doubts remain whether the rules on the identification of the beneficial owners of trusts are as clear as they could be, the reference in the ABS Guidelines to the Wolfsberg AML Principles on verification procedures in private banking could diffuse part of the problem. A similar solution could apply as far as **increased diligence** is concerned, in relation to PEP's and correspondent banking.

The rules on **record keeping** require that *"response can be provided within a reasonable time to any inquiry from the relevant authorities on, inter alia, the beneficial owner of the funds deposited with the banks"*. If this implies that financial institutions need to be able to extract expediently upon request not only information on the clients but also on beneficial owners from their entire client base, this would meet the requirements of an efficient record-keeping system. The question whether the rule really obliges banks to have computerised access to the data on beneficial owners remains to be answered.

CDSA 1999 has made the **reporting of suspicious** transactions mandatory for all persons (including non-financial institutions) and has included all predicate offences as reporting cases[64]. Furthermore, under the MAS Guidelines banks are obliged to *"clarify the economic background and purpose of any transaction or business relationship if its form or amount appears unusual in relation to the customer... or if the economic purpose of legality of the transaction is not immediately clear"*. Increased diligence is a necessary stepping stone towards notification of suspicion.

The standard set by this law obliges banks to make an STR when they know or have reasonable grounds to suspect that any property represents the proceeds of drug-trafficking or other criminal conduct. This would be the case if the transaction in question is inconsistent with the customer's known transaction profile or does not make sense economically. Failure to report is an offence under the CDSA, there is however, no mandatory blocking rule.

Singapore has changed its focus in recent years, moving away from its traditional local customer base, it is now determined to become a prime centre for financial services in SE Asia and beyond. And it has taken the first steps in response to the strong critique levied by the FATF regarding the inadequacies of its regulatory system.

On the one hand the authorities are determined to allow a controlled liberalisation of the financial markets, on the other hand they are making efforts to upgrade the AML laws and regulations, but which still have obvious flaws even in the abstract when compared to the world standard. The MAS is emphasising a change of approach from 'regulation to supervision' in order to align themselves with the newly emerging trend towards a 'risk-based approach'. The primary goal of the supervisory authority in its work on money laundering is, however, the ***preservation*** *of the Singaporean banking community's* ***reputation***[65].

63 FATF Annual Report 2001/2002 Annex B read together with page 5 of Annex C

64 Section 6 of the Notice 626.

65 MAS Notice 626, 1.1.

How this policy will work out in practice cannot yet be determined for lack of evidence. That both the authorities and the local banks are still very shy to share information even about the way in which they implement the rules with the public, does raise some serious questions, indicating that the ***'culture of secrecy'*** *has not yet been fully overcome.*

3. Switzerland: 'Reputation first'

Banking is one of the prime industries in Switzerland and is of importance to the domestic economy as well as within the international context, with asset management accounting for over half of the banks' output; of this an estimated 85% is generated by private clients. The leading position held by Swiss banks when it comes to dealing with customers domiciled abroad has also meant that international attention has been focused on the regulation of Switzerland's financial sector.

In comparison to other jurisdictions, Switzerland took an early lead in tackling the problem of money laundering, not least as a result of having to manage the 1977 Chiasso crisis. In dealing with the aftermath of this problem, the focus was on **safeguarding the reputation** of Switzerland as a financial centre. The problem was swiftly tackled and the outcome was a 'gentlemen's agreement' that was brokered between the Swiss National Bank together with the Swiss Banking Association and the Swiss banks and it became the first version of the Swiss Bankers Code of Conduct (CDB) 1977. The main focus was on private baking and thorough identification not only of the immediate client but also of the beneficial owner, shell companies and NBFIs were also included. The CDB has been regularly updated since then, with the latest version due to take effect in July 2003.

This pattern of managing a crisis to preserve the reputation of the financial centre has been typical for the emergence of AML rules in Switzerland. On the positive side though, the result was that the Swiss CDD rules were a catalyst for developments at the international level both in terms of their scope and the level of detail they required, for example with regard to ensuring the effective identification of the beneficial owner for domiciliary companies[66]: And as already mentioned[67] they have undoubtedly influenced the international developments in this area, such as Recommendations 10 and 11 of the FATF Recommendations, and more recently the BCBS of October 2001.

Criminal legislation on money laundering has consequently evolved in stages in Switzerland: The **criminal law** of 1989/90 established basic AML rules and the approach was wide from the outset with the criminalisation of the failure to exercise due diligence and a wide definition of the crime incorporating all serious offences as predicates. Money laundering is also punishable if the underlying offence was committed outside Switzerland. In 1993/94 additional criminal legislation that was rather *avant garde* covering forfeiture, organised crime and the right to notify suspicious transactions was implemented. This meant that funds under the control of a criminal organisation could independently from their source and their destination become forfeitable, introducing a rebuttable presumption of control by organised crime for those who have been convicted as helpers of a criminal organisation. Following up on a series of slow and complex procedures in mutual legal assistance, (especially relating to PEP's and the repatriation of their funds – again making crisis management a force for positive change) comprehensive reform of the MLA legislation reduced

66 Domiciliary companies neither have trading nor manufacturing operations or any other commercial activities in the country of domicile and may comprise, institutes, foundations, companies, trusts/foundations, such as Anglo-Saxon trusts, Liechtenstein foundations, and offshore companies in established in certain jurisdictions .

67 See the introduction.

the amount of appeals drastically. The new law, termed "Lex Marcos" by the media, entered into force in 1997. In 1998/99 an administrative law covering the entire AML system for banks and NBFIs was implemented.

Other additions to the law have been achieved indirectly by elevating for instance the new crime of transnational bribery to the level of a "felony", the criterion for predicate offences. So far, however, tax offences do not constitute predicate offences, since neither tax evasion nor tax fraud are ranked as felonies. In addition to intentional money laundering, the law of 1990 included an offence of lack of due diligence in identifying clients and beneficial owners, adding a criminal sanction to the already existing civil and administrative sanctions for supervised financial institutions. In the still unsupervised area of NBFI's this offence substituted regulatory law, which was eventually implemented in 1997.

Due to its gradual development **regulatory law** on AML is complex. There is to-date no single regulator, even if there are suggestions to transform the Federal Banking Commission (FBC) into a macro-supervisor, including insurance supervision and supervision of intermediaries. AML legislation distinguishes three schemes: One for regulated entities, one for unregulated intermediaries participating in an SRO and one for intermediaries directly under the supervision of the AML Control Authority in the Ministry of Finance.

The aims are similar for the entire financial services industries: Extensive CDD and KYC provisions that go into detail, whereby some of the state regulations (like the AML regulation by the FBC of 1992, revised 1998 and upgraded into an ordinance in 2003, implementing the BCBS standard of 2001) integrate industry standards, like the CDB of 1998 and give them an official status. Within the regulated segment, legal regulations cover banks, brokers, dealers, insurance companies and casinos.

Whereas supervision is strict in the core sector of financial services, the incorporation of **NBFI's** into the AML systems has been far more **arduous** – just as it has been in other countries. The laws contain an extensive formula to include NBFI's and the legal profession was included from a remarkably early date (unlike the EU which only recently tackled this issue, and the USA where it remained a taboo)[68]. Swiss lawyers are subject to the law insofar as the supply of services outside the traditional domain of legal advice and litigation is concerned. Although the Swiss legislators rapidly included NBFI's, the work load of dealing with up to 7,000 entities proved however, to be far more difficult than anticipated and the AML Control Authority initially had to face some considerable practical problems. Only since 2001 have matters started to improve and the system is beginning to establish itself in practice.

The FIU's (MROS) work has to be understood in the context of the rather atypical STR-model introduced in Switzerland by the AML-legislation of 1997: Beyond the older right to notify, the AML legislation introduced the **obligation** to notify cases of 'founded suspicion', and omission to notify is an offence[69]. The effect of notification is an **automatic blocking** of the funds in question for at least a five day period, to allow the FIU to decide on further steps. These concepts demand intensive in-house vetting of unusual cases. Whilst the numbers of notifications is relatively low, in over 80% of the cases criminal investigations are opened[70]. However, together with the new rules introducing the risk based approach in the latest ordinance by the banking supervisory authority, banks are expected

68 Art. 2 AML.

69 Art. 9 and 37 AML.

70 For 2001, 417 notifications, over 80 % led to criminal investigations.

to notify more extensively, namely where there may be an indication of terrorism[71]. Financial institutions are however in a somewhat awkward position, since they may risk prosecution if they tip-off the client.

In proportion to the rates of notification, criminal law generates relatively high numbers of cases statistically, many of which relate to domestic drug cases. International cases mostly lead to mutual legal assistance requests, where substantial sums are blocked and repatriated.

Swiss bank secrecy is not and has never been absolute, and is subject to federal and cantonal provisions regarding the banks' duty to report and testify to the authorities. Banking confidentiality is most often lifted for criminal cases such as trafficking in drugs, extortion, and terrorism, and as such, bank secrecy is not an obstacle to criminal prosecution. The fact that mutual legal assistance will not be granted for tax evasion (as opposed to tax fraud) is, however, sometimes cited as risk factor because it might offer an easy cover story for actual money launderers.

*To sum up, the Swiss system hinges on the **serious identification of clients** with CDD embedded in banking practice, which is a correlate to strong bank secrecy. Historically developments have sometimes been built on learning from past experiences, especially in the sphere of private banking. Having adopted a **broad notion of AML** in its legislation which is applied to a wide range of serious predicate offences, the Swiss have clearly gone beyond trying to deal with just drugs. The approach recognises that Switzerland is an international financial centre with private banking at its centre. On the down side, the problems with NBFIs and making CDD work in practice for this sector has caused more difficulties and is only just coming about in practice. Finally, it may be said that the primary goal of the Swiss AML system is to avert risks by tackling them early on in the account opening phase.*

4. UK: 'Active at the international level – less so at home?'

The UK's AML system appears to embody two contradictory features. On the one hand, at the **international** level the **UK** was an extremely active participant, being a driving force behind the FATF and the 1988 Vienna Convention. Whilst at that time at the domestic level, self regulation was the order of the day and interventions by supervisors were virtually unheard of, and comparatively little effort was made in KYC. This marked **discrepancy** in approach is difficult to justify given the importance of the City of London within the international financial system. It seems that early AML efforts in the UK were trained on the **collection of data** – a practice that still continues – resulting in comparatively large number of suspicious transaction reports, although whether the authorities are really able to deal with the volume produced by this 'early warning system' is open to question[72].

The prevention and punishment of money laundering in the UK is founded on a 3 tier system, much of which has undergone substantial change in recent years. First, there is the criminal law which now means the Proceeds of Crime Act of 2002, and also laws on terrorism[73]. Secondly, there are the Money Laundering Regulations from 1993 and 2001 and which are currently being redrafted and will be replaced by new regulations in June of 2003, and thirdly, there is the regulatory regime as developed and implemented by the Financial Services Authority, whose rules run parallel to the criminal laws.

The development of the **criminal law** has been piecemeal over the last two decades with serious shortcomings that made enforcement difficult (for example the standard of knowledge is subjective, which means that without an admission of guilt it is difficult to prove that the defendant knew or suspected that another had benefited

71 Art. 25 ML Ordinance.

72 Interview with representative from the National Criminal Intelligence Service (Economic Crime Unit), August 2002.

73 Especially the Terrorism Act 2000, as amended by the Anti-Terrorism, Crime and Security Act 2001, that replaced the Prevention of Terrorism (Temporary Provisions) Act 1989.

from a crime – and this has not been changed in the new law). The laws relating to forfeiture and confiscation were also problematic, again making enforcement difficult. This latter area of the law has been overhauled by the Proceeds of Crime Act 2002 (PCA) (see below). However, mutual legal assistance remains a delicate issue even after the new law and the complexities of the judicial review procedure continue, making the process slow and open to international criticism.

The Drug Trafficking Offences Act of 1986 was the first piece of legislation to address the issue of AML and concentrated on the problem of drug money laundering, in 1989 the law was further developed with the addition of terrorism related money laundering. Further extensions in 1993 to the laws were aimed at improving deterrence. However, despite these efforts, the extremely **low** number of **investigations and convictions compared to the large number of STRs**, indicated that there were serious problems with the AML system. Some of which have been tackled by the PCA , and some of which persist.

The **Proceeds of Crime Act** of 2002 constitutes the relevant criminal law and its main provisions are:

It unifies, updates and expands the existing money laundering offences[74]. It removes the distinction between the offence of laundering drug proceeds and the offence of laundering other criminal profits.

It gives powers to the police and Customs to seize cash derived from or intended for use in crime, and to secure its forfeiture in magistrates' court proceedings.

It establishes an Assets Recovery Agency. This agency will consist of a multi-disciplinary team of investigators, lawyers and accountants whose function will be to investigate and confiscate criminal assets[75]. The Director of the Asset Recovery Agency will have the power to tax an individual, company or partnership where income, profit or gain is suspected of being derived from crime.

It introduces a civil recovery scheme to recover the proceeds of crime in cases where a criminal prosecution cannot be brought against people who hold the proceeds of crime irrespective of whether they themselves are found to be guilty of any criminal conduct.

It enables assets to be frozen at a much earlier stage of an investigation. Orders to banks or other financial institutions to identify accounts of those under investigation will also be available.

Criminal sanctions include unlimited fines and a maximum prison sentence of 14 years in relation to the money laundering offences.

The PCA aims to improve international co-operation[76] in that: first, an overseas jurisdiction will no longer need to be designated that means that a mutual legal assistance treaty with the UK will not be required before restraint and confiscation co-operation can be given. Secondly, restraint will be made available from the start of an overseas investigation rather than at the point when a person is charged with an offence. And thirdly the Director of the Assets Recovery Agency will be able to deal directly with overseas requests for freezing and recovering criminal assets in civil proceedings in the same way that he can in domestic civil proceedings.

It has been said that the prime purpose of the UK 's money laundering legislation is not to outlaw money laundering but rather to ensure that suspicious transactions are reported to the authorities. This is achieved through the threat of criminal liability for failing to report[77] and the defence to criminal liability by reason of the report. Under the new laws the number of suspicious

74 PCA 2002, part 7.
75 PCA 2002, part 1 and 2.
76 PCA 2002, Section 4.
77 The penalty for failing to report is a fine or up to five years in prison, or both.

transaction reports is expected to grow even further, raising questions as to the viability of the reporting system under the new conditions.

Under the new law, suspicious transaction reporting will apply to the laundering of the proceeds of all crimes. In addition a new objective test will set the standard for reporting suspicious transactions. In practice this will mean that the Courts will look at whether an institution has followed the industry guidance such as the Joint Money Laundering Steering Group's rules.

Banks have highlighted the problems they face when making a suspicious transaction report in the context of the tipping off provisions. If they proceed with a transaction for a client when they know or suspect that the money belongs to another person they may be constructive trustees – possibly acting in breach of trust, and if they refuse to act the client may be tipped off that there is an investigation underway. These conflicting liabilities under civil and criminal law have not been resolved by the PCA. Another unresolved issue under the new law concerns the retention of the problematic subjective test relating to knowledge and suspicion in relation to the basic offences, instead of introducing an objective test of reasonableness[78].

Other concerns have been voiced in relation to using asset recovery as an alternative to a criminal prosecution, possible conflicts with Human Rights laws.

The second tier of anti money laundering regulation is to be found in the Money Laundering Regulations. Originally effective from 1994, extended in scope in 2001, they are currently being redrafted to take account of the second EU directive and are scheduled to come into effect at the beginning of June 2003.

The importance of the **1994** regulations was that they **finally introduced the obligation** on financial institutions to establish the **identity of their customers**, maintain records, report suspicious transactions and educate and train employees, in practice the issue of beneficial owners and trusts has therefore only very recently been addressed as a topic. Breach of the regulations is a criminal offence punishable with up to two years imprisonment, a fine or both, a sanction that has scarcely been applied.

The third level of anti money laundering **regulatory system** is covered by the Financial Services Authority (FSA). The FSA has amongst other duties, been tasked with reducing financial crime, and so has powers to make rules on the prevention and detection of money laundering and to institute proceedings under the Money Laundering Regulations. However the regime under the FSA is quite separate though parallel to the Money Laundering regulations and breaches of its rules may give rise to fines or the removal of authorisation to conduct business. The regulatory guidance recommended by the FSA and approved by the Treasury is issued by the Joint Money Laundering Steering Group and should be read in conjunction with the FSA's rules. This guidance is currently being updated to reflect the new law and should be available in 2003. The question remains though whether the issue of effective CDD is now finally being addressed, in particular whether the 'beneficial owner' is really identifiable. This means shifting from the traditional retail banking focus and undertaking a more detailed scrutiny of the customer.

The FSA and the government recognise that the co-operation of the financial sector is crucial to the success of anti

78 Cf. the report dated May 2000 by the Performance and Innovation Unit (PIU) of the Cabinet Office entitled "Recovering the Proceeds of Crime".

money laundering rule making. The adoption by the FSA of the risk based approach to KYC and CDD and the interaction that it has with both the financial sector and the law enforcement bodies will, it is hoped, make it more likely for regulated businesses to implement the standards. Evidence of this interaction between regulator and industry is the Statement by six UK banks on Combating Money Laundering and Terrorist Financing, published Summer 2002 (Group of Six). In this statement the banks declare that they will reconfirm the identity of all their existing customers irrespective of when they became a customer, which means customers who opened accounts before 1994. Whilst this is a positive development it does also give an indication of the inadequacies of the previous system.

The UK system of early notification of suspicious transaction reporting generates a large number of reports to its FIU[79]*. At the same time however, there is a comparatively low rate of criminal investigation and convictions. The emphasis in the UK system would thus appear to have been placed on the creation of police data with the focus on* ***'retail banking'*** *and the risks associated with* ***local drug*** *trafficking and cash related transactions. There has been an astonishing deficit relating to in-depth analysis of the concept of beneficial ownership in the Anglo-Saxon context, and therefore given this slant to UK regulation, the question is raised whether the European financial centre – the* ***City of London*** *– has so far managed to* ***evade effective AML controls****. In reviewing this question it has to be said that the recent legislative changes, in particular the Proceeds of Crime Act 2002 and moves by the industry itself (notably the* ***Group of Six*** *mentioned above), appear to signal a change in approach, as to whether it will bring about effective change, remains an open question for the time being.*

5. USA: 'From domestic drug deterrence to international terrorism'

The size and significance of the economy, its sophisticated banking system and the fact that the largest two stock exchanges (NYSE and NASDAQ) in the world are domiciled in the USA all contribute to its importance in the international arena and also in relation to the development of the AML concept.

The phrase 'money laundering' is generally acknowledged as originating in the USA, and the 'President's Commission on Organised Crime' in 1984 defined it as *"the process by which one conceals the existence, illegal source, or illegal application of income, and then disguises that income to make it appear legitimate"*[80].

Obligations to keep records and to report certain routine domestic and international transactions involving currency (Cash Transaction Reports, CTR) go back to the Bank Secrecy Act (BSA) 1970. The federal criminal offences of money laundering, however, were created as a response to combating drug trafficking. In the context of the "War on Drugs" proclaimed by President Reagan, the 1986 Money Laundering Control Act (MLCA) was adopted. The introduction of Suspicious Activity Reporting (SAR) to FinCen, the US FIU created in 1990, is more recent (1992) and is a consequence of the emerging world standard as defined by the FATF 1990. Even though the US have certainly been amongst the pioneers in developing rules against money laundering, some of the most fundamental changes have only come about very recently, with the "Patriot Act" 2001 in the aftermath of the terrorist attacks of September 11.

In a nutshell, the AML system in the US can be characterised by a very rigorous **criminal law** threatening long prison

79 In 2000 NCIS received 18,408 reports, a 27% increase on 1999 levels whilst in 2001 the figure had increased 70% to 31,251.

80 Cf. President's Commission on Organised Crime, "The Cash Connection: Organised Crime, Financial Institutions and Money Laundering", Washington DC 1984, p. 7.

sentences and drastic forfeiture as well as imposing stringent reporting requirements on the one hand, and a still rather uncharted and complex regulatory system, with an uneven coverage, relying extensively on self-regulation, on the other.

The complex structure of the basic offences in 18 USC §§ 1956 and 1957 introduced by the Money Laundering Control Act (MLCA) 1986 are easily identified as a blueprint of the criminalisation provision of the 1988 UN Convention on Drugs. § 1956 distinguishes between three separate provisions, one domestic, one on international money laundering and a separate rule criminalizing the laundering provoked by a Government sting operation[81].

The provisions basically share a common list of predicate offences referred to as "specified unlawful activities" (SUA). This list covers hundreds of US federal felonies, including violations of the Inland Revenue Code. Tax offences against a foreign state may indirectly serve as a predicate offence

The object of the crime is defined differently in domestic money laundering (proceeds of SUA) and international money laundering (monetary instruments or funds without reference to their origin!). The criminal act is defined by a list of different transactions. It is this part of the legislation that is frequently considered redundant, especially by foreign observers. Essential weight in defining illegal behaviour is placed on the subjective elements: Liability requires either intending to promote the carrying on of SUA or knowing that the transaction is designed to conceal etc. or avoid STR. The main difference between domestic and international money laundering is that the mere intent to promote the carrying on of SUA is sufficient to trigger responsibility in international transactions – even if the defendant has no knowledge of the illicit origin of the funds.

§ 1957 adds yet another variation to the list of criminalized activities: The knowing engagement in a monetary transaction. Even if there are fine differences between the provisions, there is a considerable amount of overlap.

Ancillary offences further criminalize violations to the BSA, namely the "failure to file CTRs", "structuring transactions to evade reporting requirements" and the just amended operation of "illegal money transmitting businesses" (targeting Hawala banking) as well as the new offence of "bulk cash smuggling".

Conviction statistics indicate that over the last few years a stable figure of around 1000 defendants were sentenced to prison each year for Money Laundering. This statistic evidently does not take sanctions against legal persons into account.

The **Civil Asset Forfeiture Reform Act** (CAFRA) 2000 has dramatically expanded the list of crimes subject to civil forfeiture to include all SUAs. Civil forfeiture is a procedure *"in rem"* with a different evidential standard to criminal forfeiture. Innocent owners may claim relief, however, the rules have been toughened up recently: After CAFRA the claimant bears the burden of proof.

Criminal forfeiture is directed at the defendant and follows the general rules of evidence in criminal matters. Unlike civil forfeiture it, however, does not require a nexus between the property and the underlying offence: The property forfeited may serve as a substitute to products of the offence transferred out of the reach by any means.

Similar to UK law, a court order requiring similar prerequisites to those of a search warrant is necessary for a restraining order under US law.

81 18 U.S.C. §1956 (a)(3).

Statistics on civil and criminal forfeiture for 2001 indicate that $241 million have been forfeited in connection with money laundering offences including both civil and criminal forfeiture, a figure relatively small compared to the economic significance of the US economic centre and the dimensions of the problem.

With Executive Order 13224 of 25 September 2001 President Bush blocked all property and interests in property of originally 27 individuals and entities suspected of terrorist involvement (to which others were added later on)[82]. The scope of the order covered all property interests of these persons in the US and within the control of US persons, including overseas branches. Additionally, the Order exerts pressure on **foreign** financial institutions, threatening to block their property if they are found to assist terrorism in any way. The Executive Order is remarkable both for its extraterritorial approach and the strict liability it introduces.

Even though the US has concluded bilateral MLA and extradition treaties with many countries to assist foreign states in investigations on money laundering, a treaty does not seem to be required and judges may be directly approached with requests for assistance.

Like other common law countries, the US does require "probable cause", at least for extradition. The extradition of laundered funds is treated as an issue of sharing of seized assets. It remains open whether – beyond the cases where countries co-operated in the seizure of defrauded, embezzled or stolen goods are actually restituted to the victim abroad integrally, even if the victim is a foreign state.

The basic obligations to maintain **CDD**, to file SARs and to develop a compliance programme **apply unevenly to different sectors of the financial industry**. Even though the BSA had allowed the Treasury to go much further, the Secretary of the Treasury had until very recently only subjected the four core types of financial institutions to the full AML rules (banks, securities broker-dealers, money services businesses and certain gaming establishments). A further group of three types of institutions is only subject to CDD-rules.

A long list of NBFIs are exempted from AML rules, even though the US has already been harshly criticised for it in the 1997 FATF evaluation[83]. The Treasury has very recently expanded CDD and reporting requirements to some of the NBFIs in its regulations implementing the Patriot Act[84]. However, attorneys, notaries and unregulated fiduciaries are still not subject to the AML reporting and CDD rules. It would rather stretch the general meaning of the words self-regulation or 'risk-based approach' to apply them to this type of regulation.

Until 2001 the statutory obligations on KYC had merely requested companies to make *"reasonable efforts to be reasonably certain of the identity of their customers"*. The Patriot Act and the new regulation by the Treasury Department impose more specified duties on an extended group of financial professions to implement customer identification programmes (CIPs). **Beyond a basic minimum the regulation remains purely exhortative.** The focus is very much on account opening procedures, an explicit requirement for ongoing monitoring is not foreseen. It may, however, be deduced from the risk-based approach. Overall, the decision how to proceed if a financial institution *'cannot form a reasonable belief that it knows the true identity of a customer' is left open.*

The issue of material identification ("CDD" in a narrower sense, including, for instance, the gathering of information on occupation, nature of business etc.) beyond formal identification

82 See 2002 NATIONAL MONEY LAUNDERING STRATEGY at 1. As the Report notes, "[t]he 2002 National Money Laundering Strategy breaks important new ground, and, for the first time, describes a coordinated, government-wide strategy to combat terrorist financing. We will apply the lessons we have learned from the federal government's efforts against money laundering to attack the scourge of terrorism and to deny terrorist groups the ability to finance their cold-blooded murder." Id.

83 FATF Second Mutual Evaluation Report on the United States, 21 March 1997 (Confidential).

84 Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act 2001.

has so far only been addressed in ABA Recommendations[85]. Their legal value does not so far seem to go beyond private best practice suggestions.

Overall the system is very much focused on **retail banking** and restricts itself to a mere minimum of mandatory rules. This impression is corroborated by the lack of a general rule obliging financial institutions to determine beneficial ownership. This rather remarkable divergence from the internationally agreed standards has been criticised by international organisations[86]. An explanation would have to take the overall thrust of the US AML system into account, which from the outset has been directed against drug money, especially cash and the first stage of money laundering, the so-called 'placement' as opposed to the "layering" and the "integration" stages[87].

Only after September 11 was the administration able to override industry concerns and introduce elementary requirements on the identification of **beneficial owners** and on determining the source of funds, though still restricted to private banking. However, even those rules only apply to funds held for non-US-persons. Apart from falling beneath the international standard, this restriction to foreign persons raises serious questions about the effectiveness in determining money launderers and terrorists: As long as terrorists are US citizens or use US stooges, they will easily elude detection. It is remarkable that the discriminatory treatment of US and non-US persons seemed politically more essential than maximising effectiveness even after September 11.

In a closely related area, however, the Patriot Act and its implementing regulations go beyond previous standards: in **correspondent banking**. Because the "Bank of New York" and other scandals demonstrated frequent abuses of correspondent banking relationships as a way to infiltrate the US financial industries, this issue was singled out for strict Government regulation. Enhanced due diligence standards apply to accounts owned by foreign banks operating under an off-shore banking licence or a licence issued by a jurisdiction designated as non-cooperating in international AML-efforts by the Treasury Department or by an inter-governmental AML-organisation such as the FATF. Relations to foreign shell banks are to be phased out. In general, banks must ascertain the ownership, the reputation and the adequate supervision of respondent banks. The issue has since been picked up by international standard setters[88] and by the industry itself[89].

The Patriot Act has expanded the scope of **reporting requirements** to include SEC registered brokers and dealers. The extension of other professions is being contemplated. Some of the professions under obligation to identify clients are still not required to report suspicion, and this includes lawyers.

For those professions covered, reporting requirements are rather broad, focusing on "activities" rather than on mere transactions. However, the definition of suspicious activity is left to the individual institutions to be translated into operational terms. The procedural rules on notification clearly anticipate that up to 95 % of SARs will be made in the aftermath of transactions, without need of urgent intervention. Banks are given a 30-day-period to report from the initial detection of the facts; and they may delay filing for another 30 days if no suspect was identified at the time, in order for one to be identified.

85 See, e.g., American Banking Association, Industry Resource Guide – Identification and Verification of Accountholders (Jan. 2002), available at http://www.aba.com/aba/pdf/InsResourceGuide.pdf) (last visited Nov. 1, 2002).

86 See the critique of the FATF in its 1997 Report.

87 Cf. internal report by US Customs to the Subgroup Statistics and Methods of the FATF 1989.

88 BCBS, FATF.

89 See the Wolfsberg Principles.

Similar leeway for bureaucratic processes is left on the Government side, allowing 10 days for computer processing. There is no automatic blocking of the funds. Only in the remaining 5 % of cases is immediate action by telephone etc. required.

It appears that the system is basically aimed at **gathering data** and looking out for **recurring patterns** and conspicuous client behaviour. Similar to the UK approach it is primarily focused on retail banking and mass-notification of unusual, rather than genuinely suspicious activities. In 2001 roughly 204,000 SARs were filed; in 2002 the figure was raised above 240,000. Again the number of criminal investigations, let alone convictions, is much lower. Inferences on the effectiveness of the system cannot be drawn directly from these figures. But they help to give an understanding of the diverging approaches.

*Overall the US AML-system continues to be **preoccupied with cash** generated by illegal drug-trafficking and the first stage of money laundering, the placement phase. To this was added the issue of terrorist financing. Again, however, the emphasis is on structuring of small transactions, on cash smuggling etc. The US regulatory system does not really address the considerable vulnerability of its financial centre to abuses for large-scale "layering" and "integration" purposes. Instead the system **relies on deterrence** through tough criminal laws and stiff "civil and criminal" forfeiture rules. The criminal justice system is nourished by extensive reporting of suspicious activities. In comparison – especially with European systems – the **regulatory standards remain astonishingly undefined** with many types of financial institutions within the scope of international standards left outside CDD, reporting or compliance obligations. As a consequence the notion of self-regulation is correspondingly well developed, and official guidance is given only in specific areas (for example correspondent banking and PEPs). In particular the **identification of beneficial owners is not yet current standard**. The new rules contained in the Patriot Act 2001 still differentiate between US and non-US persons.*

Conclusion: The case for convergence

The seemingly contradictory policy of re-regulation of financial intermediaries juxtaposed with markets that have undergone extensive liberalisation in a world where financial centres serve the needs of globalisation, can in fact be rationalised: In order to control the abuse of financial centres by transnational criminal operators, preventive and punitive measures are clearly necessary. Moreover, the stability of financial markets has to be secured from the damage that could result through systemic misuse. This latter aim has meant that international bodies such as the Basel Committee, the FSF and the FATF amongst others, are continually developing details for a harmonised approach aimed at preventing "money laundering".

The standards that are implemented at the national level in response to these international principles and recommendations, are evaluated and peer pressure is strong internationally, even if the agreed criteria essentially aim at formal compliance with the letter of the standard rather than at genuine effectiveness of the measures. The tragic events of September 11 have not changed the methodology, but have served to extend the applicability of the standards and heightened the pressure to conform at the national level – whilst the international approaches still lack coherence despite a seemingly united stance towards the problem.

Although national systems all address the same elements associated with the problems of money laundering, they diverge considerably in their emphasis. It may be suggested that the substantive mix of AML rules – even if their historic evolution is different in each of the countries examined – reflects a tacit, but at the same time, defined agenda: The various systems are in need of interpretation.

It emerged that the two large financial centres (**USA** and **UK**) placed far more emphasis on an **'early warning system'** with the recording of everyday transactions and the reporting of unusual or suspicious circumstances within the context of retail banking. Having collected information, its primary use was not so much to initiate criminal proceedings, but more to build up a databank of intelligence for future strategic and tactical use by the police or similar authorities. In both countries the emphasis on criminalisation of money laundering was far stronger than on the preventive approach of customer identification. In fact, the **lack of effective in-depth identification of customers and beneficial owners** (especially where corporate vehicles and trusts are used) and the reluctance to have this data available for law enforcement (documentation obligation) could support the contention that the effect of these systems is **comparable to "bank secrecy"**: Instead of protecting information on clients, neither system really wants to know or establish these details at all. Broadly speaking, the anti-money laundering concepts in the UK and the US are to-date more attuned to the risks posed by domestic drug markets, cash and suspicious "placement" in high street banks rather than the illegal world-wide financial circuit which would mean the additional burden of equipping their systems against the latter phases of money laundering.

Both in **Singapore** and **Switzerland**, the AML-systems are far less oriented towards data collection for intelligence and law enforcement purposes. In Switzerland the system relies on **in-house vetting** of clients. Suspicious transaction reports are fewer than in the UK and USA (even in relative terms), but in Switzerland at least, they lead in most cases to the opening of a criminal investigation. The main emphasis is placed on CDD and KYC, and considerable efforts are made in screening clients in the account opening phase although there is no obligation to notify account openings that are abandoned in the formative stage by the financial intermediary. The main emphasis by these countries is to **keep risks away** from their relatively small but somewhat exposed financial centres. Extensive KYC has a direct correlation to strong banking secrecy. Whereas the Swiss approach is a product of managing various crises, the policy in Singapore is recent and has involved deliberate moves to make the financial centre compatible and attractive for international business.

Meanwhile, looking beyond this state of affairs at the domestic level, regulators (especially with the BCBS) and exponents of the industry (Wolfsberg Group, Group of Six, ABA, SBA etc.) **are striving towards harmonising the approaches**. The latter within their specific industry segments whilst the regulators are primarily addressing themselves to their member states. In certain subject areas both the private sector and the international organisations define concrete rules (such as for PEP's and correspondent banking), and overall they now increasingly adopt the "risk-based approach" delegating it to the micro-level of the private sector to define risk categories and the appropriate internal measures. This may result in a grey area between where the rule based approach leaves off, and the margin for defining risk commences. The harmonisation of risk strategies also requires further development of a common vocabulary and agreed definitions so that effective standards that really contribute to a level playing field are developed. As for the experiment of the risk based approach and the relationship it creates with the financial services industry, so far it is an untested one: This combination of partnership, delegation and empowerment between government and industry may turn out to be a creative and solution oriented approach or it may be grist for the lawyers mill should shortfalls in risk coverage occur.

However, as a consequence of applying the risk based approach, all major banks are introducing computer-based filtering mechanisms for retail clients and more individualised mechanisms for private banking. It may be expected that some systems which have **over performed** in comparative terms may be able to reduce their efforts (such as Swiss banks on identification of beneficial owners in retail banking), whilst **others will have to catch up (US banks on KYC in private banking)**. And although the **differences** amongst the larger players are **rapidly disappearing**, smaller institutions and especially NBFI's have still to find their way in the changing regulatory landscape.

Overall, to give a simple answer to the question whether the 'playing field is level in AML regulation' in the various financial centres described here, the response would be that it is not level but neither is there a major misbalance: Switzerland for example looks to preserve reputation by early identification of the client but could be criticised for not catching criminals, whilst the UK makes a hue and cry about the need to apprehend criminals whilst ignoring the sophistication of its financial centre and its attractiveness for international money laundering. In short there are deficits and incongruent features in all systems. At the international level in terms of 'soft law' (such as the BCBS) and private initiatives (like the Wolfsberg Banks) there may in 'formal' terms be a level playing field, but without effective monitoring processes capable of addressing application in practice, they also display their limitations.

Customer Due Diligence-Overview

Mathias Pini

The information contained herein is largely drawn fom the study conducted by the Basel Institute on Governance commissioned by the Stiftung Finanzplatz Schweiz, Towards a Level Playing Field in Cross Border Banking: Comparing Anti-Money Laundering Rules (UK, USA, Singapore, Switzerland), presented in January 2003. For abbreviations see separate list.

TOPIC	SWITZERLAND	U.S.	UK	SINGAPORE
SCOPE OF APPLICATION OF KYC RULES / ADRESSEES	**According to Art. 2 MLA:** Banks, managers of funds, insurance institutions, securities traders, persons who on a professional basis, keep on deposit or help invest, transfer assets belonging to third persons, particularly persons who undertake credit transactions (including consumer credit or mortgages, factoring, financing of commercial transactions or financial leasing), who provide services related to payments, including electronic transfers on behalf of third parties, who issue or manage means of payment such as credit cards and travellers checks, who trade in bank notes or cash, money market instruments, currency, precious metals, who offer or distribute shares in funds, in the capacity of distributor of a Swiss or foreign investment fund, who undertake asset management, make investments as investment advisors, keep or manage securites.	**BSA/Treasury Department AML-Regulations:** Banks, securities broker-dealers, money services businesses certain casinos. **PA:** Credit unions, mutual funds, futures commission merchants etc. **Not covered** are e.g. private bankers (except to the extent covered by enhanced DD requirements for private banking accounts), insurance companies, attorneys and notaries. Some institutions are subject to **KYC** AND **SAR**, others **ONLY to KYC**.	All individuals and firms engaging in investment business within the meaning of the Financial Services and Market Act 2000. 2nd EU Directive will be implemented by the revised ML Regulations expected in June 2003. Adherence to the JMLSG Guidance Notes that have been approved by HM Treasury must be taken into consideration by the courts when considering whether a ML offence has occurred under statutes or whether the Regulations have been breached **(JMLSG Guidance Notes currently under revision due June 2003)**.	The Monetary Authority of Singapore **(MAS)** has issued six separate **Guidelines** on Prevention of ML to the financial sectors, such as: ■ Banks ■ merchant banks ■ finance companies ■ life insurers ■ dealers and investment advisers ■ futures brokers, futures trading advisers and futures pool operators. The respective contents are almost identical in substance. (The following remarks refer to Guidelines issued to banks). Guidelines must be applied by overseas offices.
DIRECT CUSTOMER	Identification procedure in Switzerland is left to self regulation. The applicable self regulatory instrument for banks is the CDB (latest version CDB 03, effective as of 1 July 2003). Identification required. **Individual person:** official identification document (e.g. passport) with a photograph. **Domestic legal entity:** extract from the commercial register or similar document e.g. "Schweizerisches Ragionenbuch", public websites, such as www.zefix.ch, all not older than 12 months. **Foreign legal entity:** ID is verified by means of an extract from the commercial register or an equivalent document or extracts from public websites for	BSA embodies various KYC principles. Duty on regulated financial institutions to take reasonable efforts to be reasonably certain of the identity of their customers and BO. Expanded KYC principles due to PA: Implementation of KYC programs (CIP). Special: Screening of customers against government lists of known terrorists is mandatory.	It is required that the FI obtains **sufficient evidence** of the identity of the customer. FI must adopt a risk-based approach to determine what is reasonable to obtain sufficient evidence of identity. (e.g. for **UK resident private individuals:** name permanent address, date of birth, passport, driving licence, local authority tax bill etc. / for **Non UK resident private individuals:** passport, permanent residential address from the best available sources) The process must be cumulative.	Satisfactory evidence of the ID and legal existence of persons applying to do business with the bank. Following information must be obtained: Name, permanent and mailing address, date of birth, nationality (original documents shall be requested).

TOPIC	SWITZERLAND	U.S.	UK	SINGAPORE
DIRECT CUSTOMER	commercial register entries or equivalent document, substantiating the existence of the legal entity or company (such as certificate of incorporation). (Cf. also non face-to-face clients).			
BENEFICIAL OWNER	Establishing of BO **required, if not identical** with direct customer. Establishing of BO **in any case:** in unusual circumstances (e.g. when a power of attorney is conferred on someone who evidently does not have sufficiently close links to the contracting partner, if the submitted assets are disproportionate to the persons known financial standing), non face-to-face account opening for an individual (CDB 03 Note 26, cf. also *exceptions*), collective accounts (with exceptions for certain FIs, cf. *introduced business* and *professional secrecy*), domiciliary companies according to Art. 4 CDB 03.	BSA does not impose a separate obligation on FI to ascertain the identity of the BO other than the standard requirement to implement sufficient procedures to be reasonably certain of the identity of the BO. Identification of BO only required for private banking accounts held by or nominated for non-U.S. persons.	Identification evidence should be obtained for any known BO who is not a signatory, or named investor.	ID required if BO not identical with direct client but only in the ongoing relationship (MAS 6262, 4.3). Apparently the customer must be asked about the BO already at the stage of account opening, but it is not mentioned directly (in MAS 6262, 4.1 there is only an obligation to check whether an applicant claiming to act on another person is *authorised* to do so). If there is an intermediary and if the intermediary is supervised (either by a Singaporean authority or by an overseas regulatory authority withequivalent standards) a **written assurance** about the evidence of the identity of the BO is required. If the intermediary does not fall into one of the mentioned categories, **satisfactory evidence** is required. (MAS 626, 4.21) Cf. the cross reference to the PB sector (ID always required).
CORPORATE VEHICLES/TRUSTS	**In general:** Extract of a public register required or equivalent documents. (cf. direct customer) **Publicly registered companies:** ID not required (because knowledge of identity is publicly available). **Domiciliary companies and trusts:** Extract of the commercial register or equivalent document (e.g. certificate of incorporation). Especially for trusts: construction must be understood, founder, potential beneficiaries, persons with the power to instruct must be identified; distinction between different types of trusts according to the risk of abuse (discretionary, revocable trusts).	Documents required showing the existence of the entity, such as registered articles of incorporation, government-issued license, partnership agreement, or trust instrument.	**In general:** registered number, registered corporate name and any trading name used, registered address, directors, its owners and shareholders, nature of the corporation's business (FI decides on how much documentary evidence is needed). **Lower risk corporations:** info about the company's incorporation and registered address, list of shareholders and directors **Higher risk corporations:** identity of all persons with a significant interest in the company (20% and more) must be verified, evidence of the principals, BO and anyone else with a	Very detailed regulations with respect to corporations, trusts, clubs, etc. Copies of certificate of incorporation etc., appropriate directors resolution. Satisfactory evidence of intermediaries and authorised signatories. Enhanced DD with shell companies (shell banks not explicitly banned).

TOPIC	SWITZERLAND	U.S.	UK	SINGAPORE
CORPORATE VEHICLES/TRUSTS			principal control over its assets. IBC that are registered in an off-shore jurisdiction, but operate from another jurisdiction, must be followed with particular attention. **Registered public companies:** copy of the latest corporate report and accounts or its file at the Registrar of Companies, certified copy of the resolution of the Board of Directors to open the account. **Credit and Financial Institutions:** ID not required for UK or EU regulated Companies. For Non EU countries confirmation of the existence through home country Central Bank or supervisor, subsidiary, branch or correspondent bank. If located in an NCCT, applicable procedures for non-financial companies are applicable. **Trusts:** Distinction between low risk and high risk trust. ID of those providing funds, i.e. settlor(s) and those who are authorised to invest, transfer funds, or to make decisions on behalf of the trust, i.e. the principal trustees.	
WALK-IN-CLIENTS/ THRESHOLD	Identification and establishing the BO above a threshold of CHF 25,000 (no smurfing). In cases of doubt ID/BO is required below threshold.	Currency Transaction Reporting (CTR) system, threshold of US $ 10,000; no other specific ID requirements for walk-in-clients.	ID for one-off transactions above a threshold of Euro 15,000.	ID above threshold of S$ 20,000 and for safe deposit facilities.
NON FACE -TO-FACE CLIENTS	For individual clients (domestic and foreign): Passport/ID required or a certified copy of an identification document (can be issued by a branch of the bank, a correspondent bank [if specifically appointed], a notary public or another public office that customarily issues such authentications). The ID based on an official ID-document at delivery or receipt of mail is also deemed as sufficient proof of identity, provided that personal delivery to the recipient is thus warranted.	Correspondent accounts are identified as being a conduit for laundered funds. PA requires enhanced DD to be conducted for certain correspondent accounts maintained on behalf of a **foreign bank**, especially for accounts owned by foreign banks operating under an offshore banking licence or a license issued by a jurisdiction designated as a NCCT. Enhanced procedures include taking reasonable steps to ascertain the identity of each of the owners of the foreign bank, to conduct enhanced scrutiny	Supplementary procedures must be undertaken. Important to ensure that the applicant is who s/he claims to be. Procedures to identify and authenticate the customer should ensure that there is sufficient evidence to confirm address and persona identity and at least one additional check to guard against impersonation fraud. Different procedures for UK resident private individuals, non UK resident private individuals and corporate clients.	KYC must be as stringent as for a FTF verification. Number of checks that should be undertaken: Telephone contact with the applicant at an independently verified home or business number, verification with the applicants employer (if consent), salary details on recent bank statements, reliance on CB information, a copy of passport may also be required to be submitted.

TOPIC	SWITZERLAND	U.S.	UK	SINGAPORE
		of the account and to ascertain whether the foreign bank provides correspondent accounts to other foreign banks, and if so, to identify such foreign banks.		
E-BANKING	Same rules apply as for NFTF clients. According to the **new ML Ordinance** e-banking is considered as a client relationship without any personal contact, hence it has to fall under the category high risk customer (requiring enhanced DD).	The FI must have procedures in place for conducting verification when documentary evidence is not available.	No reference, but likely to be covered in new JMLSG Notes June 2003.	Cf. Non face-to-face clients
VERIFICATION OF IDENTITY	Yes with respect to direct client (original documents or confirmation of authenticity). With respect to BO the bank relies on the particulars provided by the direct customer (Form A). However the banks have the discretion and the right to print their own forms.	If KYC is required, verification is also required.	Sufficient identification evidence must be obtained. Verification procedures follow a RBA.	Verification is required.
CUSTOMER PROFILE	Customer profile is required according to the ML Ordinance. Profile must follow a RBA (cf. *risk categories*).	Due to the lack of the duty to report suspicious activities of (cf. SAR) of several FIs a customer profile does not seem to be required under the AML Legislation, even though industry practice may require it.	No reference but pre-condition for a STR.	No reference but pre-condition for STR. ABS-Guidelines mention a "customer's transaction file" (6.1) and oblige banks to clarify the economic background and purpose of transactions, hence a customer profile seems to be required.
ONGOING MONITORING	Required and forms a very important part of CDD.	The BSA does not require ongoing monitoring or periodic updating of client information by subject institutions, but rather focuses on their obtaining and verifying information in connection with account opening procedures.	Not addressed in the JMLSG Guidance Notes.	Obligation to clarify the economic background and purpose of any transaction or business relationship. Even though not explicitly mentioned it must be a pre-condition for STR. With respect to PB the ABS Guidelines refer to the Wolfsberg Principles, which oblige banks to implement an explicit monitoring program.
DOCUMENTATION	Is required in a form that the internal auditing department and the external auditing firm are in a position to verify that the ID procedure and BO have been established.	Required and expanded by PA.	Required.	Internal end external auditors must be able to judge compliance with the guidelines. Banks must satisfy within a reasonable time any enquiry or order from the relevant authorities.

TOPIC	SWITZERLAND	U.S.	UK	SINGAPORE
SAR	Every FI subject to AML is also subject to SAR obligations. Notification when knowledge or founded suspicion. The new ML Ordinance refers to terrorism and requires a notification when the background information reveals a link to a terrorist organisation or terrorist financing.	Only some FIs are subject to SAR (others only to CIP). SAR when a FI identifies ("knows, suspects, or has reason to suspect") a suspicious financial transaction or pattern of suspicious behaviour. Banks and securities brokers must report ST only if transaction totals US$ 5,000 or more. Money services businesses must report if the ST totals US$ 2,000 or more.	STR applies to laundering proceeds of all crimes. Obligation to report knowledge or suspicion of money laundering. In addition under Proceeds of Crime Act 2002 there is a new objective test for STR.	Each bank shall institute a system for reporting ST. The obligation to report is on the individual. A transaction is considered as suspicious if the transaction in question is inconsistent with the customers known transaction profile or does not make economic sense.
EXCEPTIONS OF ID	No ID for cash transactions of walk-in clients or execution of transactions with securities, currencies as well as precious metals if not exceeding a threshold of CHF 25,000. It is not necessary to formally verify the ID of a contracting partner when opening a account in the name of a minor [if not exceeding a threshold of CHF 25,000], a rent guaranty account, an account a view to paying up capital stock, if the identity of the contracting party is publicly known (public company).	CTR System for transactions over US$ 10,000.	■ Existing clients before 1 April 1994 (However cf. the joint statement of principles of the six leading UK banks, they agree to "reconfirm the identity of [our] existing customer, irrespective of when they became a customer." ■ Applicant is a UK or EU Credit institution or FI. ■ For one-off (single or linked) transactions under Euros 15,000. ■ For the introduction of one-off transactions from overseas. ■ For small life insurance contracts and long term insu rance business policies with respect to occupational pension schemes. All exceptions do not apply if there is knowledge or suspicion of ML.	Under threshold of S$ 20,000.
DELEGATION	Delegation of KYC (with respect to contracting partner and BO, according to CDB) is possible, if the mandatory has been ***elected*** (written agreement) and ***instructed*** properly and if the bank is able to ***control*** the realisation of the contractual duties. Under the same conditions additional investigations (cf. Art. 17 and 19 ML Ordinance) can be delegated to third parties.	Delegation is possible, but does not exempt the FI from its ultimate responsibility.	No reference.	No reference.

TOPIC	SWITZERLAND	U.S.	UK	SINGAPORE
CORRESPONDENT BANKING	According to the CDB 03 the BO in principle must be identified for all accounts. **Exceptions:** BO must not be identified if the account holders are banks or investment banks (domestic and foreign) and other financial intermediaries (domestic FIs according to MLA; foreign FIs only if subject to an adequate supervision). The bank must require banks or other FIs to submit a declaration of the BO or take other measures if it has cause to assume misuse. No relationship with shell banks are allowed.	PA requires FI to establish procedures to conduct enhanced DD for certain correspondent accounts maintained on behalf of a foreign banks, especially for banks operating under a offshore banking license or a license issued by a NCCT. Each of the owners of the-foreign bank must be identified. Knowledge, whether the CB provides services to other foreign banks, if yes, identifiation of such banks required. NO shell banks.	RBA to know your corespondent's procedures to ascertain whether correspondent bank is itself regulated for ML prevention and if the correspondent is required to verify the identity of its customer to FATF standards. Where this is not the case, additional DD will be required.	No reference.
INTRODUCED BUSINESS AND PROFESS-IONAL INTERME-DIARIES	Cf. *Correspondent Banking*. No notification of the BO necessary, if the account is held by a FI subject to an adequate supervision.	No reference.	Distinction between **Introduced business** (intermediary introduces a client who then becomes a C himself) and **professional intermediary** (where the Intermediary is the customer himself). ■ Underlying company must be identified. ■ If FI relies on introducer , introducer must complete a introduction certification (accompanied certified copies of the identification evidence that has been obtained). ■ Reasonable measures must generally be taken for the purposes of establishing the identity of any person on whose behalf an applicant for business is acting. If agent is in an FATF mem ber country, an assurance from that applicant that it has identified its principal and kept records will be sufficient. ■ Distinction between omnibus accounts for multiple clients and accounts for specifically one client. ■ ID of introducer required, if not UK or EU firm. ■ BO must only be identified, if introducer not from EU or UK ■ Solicitors (cf. professional secrecy). ■ Private companies ID is obtained for the principal underlying BO(s) and those with principal control.	Detailed rules in the ABS-Guidance (4.8). Intermediary (=customer of bank) opens a bank account on behalf of a third party (third party is BO). **If intermediary is regulated by the MAS:** Where the applicant intermediary is a FI regulated by the MAS or is a subsidiary of such an institution, it will suffice for a bank to rely on the applicant's verification of the identity of the underlying principals or beneficiary in establishing a banking relationship. **If foreign FI (not regulated by MAS):** Same rule as for MAS controlled FI, if FI supervised by a foreign regulatory authority from a member country of FATF (intermediary must file a written assurance that evidence of the underlying principal or BO has been obtained). **Non-financial institution intermediary:** ID of BO must be evident as well as source of funds and legal authority to act as intermediary. An intermediary form must be filed.

TOPIC	SWITZERLAND	U.S.	UK	SINGAPORE
				Trustee, nominee and agent account: Bank must ascertain whether an applicant is acting as trustee nominee or an agent on behalf of a third party before establishing a banking relationship. Besides establishing the ID of trustee, nominee or agent, bank **must** establish ID of BO.
PROFESSIONAL SECRECY	Special case provided for attorneys and notaries to fill in the Form R: no notification of the BO if the account held by a notary or attorney is in connection with the core business, i.e. the business covered by legal privilege. Attorneys and notaries must, however, communicate the exact type of business.	Attorneys and notaries are currently **not covered** by the AML system in the U.S. (but may be revised in the near future).	Solicitors: FI must take commercial decision whether they conduct business without knowing the BO.	Business with solicitors and lawyers is not banned. However the bank should not be precluded from making reasonable enquiries if any suspicion is aroused. Law enforcement agencies will seek information directly from the intermediary as to the identity of its client and the nature of the relevant transaction.
RISK CATEGORIES	Bank must assess the risk linked to a client and define the relevant risk categories. The **ML Ordinance foresees** various risk categories, e.g. ■ Amount of assets ■ Flow of funds ■ Domicile or residence of customer or BO ■ Place of incorporation of companies or trusts ■ Type and place of business ■ Type of accounts.	Not explicitly mentioned, but certain types of customers or transactions need enhanced DD. Therefore risk categories are surely helpful (but most likely up to the individual FI).	No reference.	ABS Guidelines refer to Wolfsberg Principles which emphasise risk categories.
RISK BASED APPROACH	**ML Ordinance:** Heavy emphasis on the RBA. Banks must assess the risks posed by their clients and react correspondingly. The CDB on the other hand provides solely a minimal standard, i.e. contains no reference to the RBA.	US system seems to put more emphasis on self regulation, information exchange and customer screening against terrorist lists, than a RBA. Certain risk factors (such as attorneys, domestic private banking clients or insurance companies) are not covered by the AML system. However, a RBA is also considered to be crucial (e.g. the verification of the collected information must follow a RBA).	Heavy emphasis on the RBA. RBA used to determine the information to be collected to identify the client or the additional information that is required to know the nature of the business.	ABS Guidelines refer to Wolfsberg Principles which strongly support the RBA.

TOPIC	SWITZERLAND	U.S.	UK	SINGAPORE
PEPS	Due to scandals in the past there is a big emphasis on the topic. According to the ML Ordinance PEPs are considered as high risk clients leading to the high risk categorisation in the **ML Ordinance**. The PEP Working Paper 2001 of Supervisors is considered as the basis in handling the relationship with PEP clients.	PA requires that private bank accounts held by senior foreign political figures, members of their families, and their close associates require enhanced scrutiny.	PEP-issue not explicitly mentioned: Nevertheless the identity of foreign nationals must be established and enhanced scrutiny must be conducted in relations with clients from under-regulated countries.	ABS Guidelines refer to Wolfsberg Principles which set out detailed rules with respect to PEPs.
PRIVATE BANKING	PB is not explicitly mentioned, but the risk categories in Art. 17 ML Ordinance cover the essential scope of PB business (value of the assets, origin of clients, type and place of business, lack of personal contact etc.).	PA requires enhanced DD of PB accounts held by or maintained for non-U.S. persons, including foreign individuals visiting the US, or a representative of a non U.S. person. PB Account is defined by the PA: ■ Minimum deposit of US$ 1 Mio. ■ Account opened on behalf of one or more individuals with a direct or beneficial interest in the account. ■ Managed by an officer or agent of a FI.	Additional information or documentation is required (because purpose and expected level of use may not be immediately apparent).	ABS Guidelines refer to Wolfsberg Principles designed for private banking.

Customer Due Diligence-Overview

Mathias Pini

For abbreviations see separate list.

TOPIC	Basel Committee on Banking Supervision, October 2001 (BCBS)	WOLFSBERG AML PRINCIPLES, May 2002	FATF 40 Recommendations, 1996 and the Public Consultation Paper of review for the FATF 40 Recommendations, May 2002
SCOPE OF APPLICATION OF KYC RULES / ADDRESSEES	Addressed to bank supervisors around the world. The expectation is that the presented KYC framework will become the benchmark for supervisors to establish national KYC-practices. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies. BCBS states, that there is a need to implement similar guidance for all non banking financial institutions (NBFI) and professional intermediaries of financial services, such as lawyers and accountants.	Private initiative by 12 banks with substantial percentage of private clients. Principles are considered to be a gentlemen's agreement for member banks. The aim is to provide an important global guidance for sound business conduct in international private banking.	**40 Rec. (1996)** Addressees are governments of member countries. Financial institution (i.e.) banks and also NBFIs [Rec 8/9 including an Annex listing financial activities undertaken by non FIs]. FIs must apply and implement the 40 Rec. also to their subsidiaries and branches abroad. **Review 2002–2003** Definition of FI by reference of a range of financial (and functional) activities (rather than legal form or entity). Persons or entities engaged in financial activity with an amended list of activities are covered. It is the FATF's aim to cover all persons or entities that conduct commercially "financial activities" even if only ancillary to their main business. Proposed extension to several categories of non-financial businesses and professions, such as casinos, dealers in real estate, and high value items, lawyers, notaries, accountants and auditors, investment advisors.
DIRECT CUSTOMER	Identification of direct customer (person or entity) is absolutely essential. cf. also the General Guide to Account opening and Customer Identification, Attachment to the BCBS, dated February 2003.	Identification of direct customer (person or entity) is absolutely essential.	Identification of direct customer (person or entity) is absolutely essential
BENEFICIAL OWNER (BO)	■ Identification of any person on whose behalf an account is maintained (i.e. BO). ■ Identification of beneficiaries (for transactions conducted by professional intermediaries). ■ Identification of any person or entity connected with a financial transaction that can pose significant risk (to the bank).	BO must be established for all accounts, i.e. for natural persons, legal entities, trusts, unincorporated associations.	**40 Rec. (1996)** BO must be established but the language about precise obligation not very clear. **Review 2002–2003** ID of BO and the person(s) that have the control over direct customer or funds or on whose behalf a transaction is being conducted.
CORPORATE VEHICLES/TRUSTS	cf. also the General Guide to Account opening and Customer Identification, Attachment to the BCBS, dated February 2003. A bank should understand the structure of the **company**, determine the source of funds, and identify the BO and those who have control over the funds. For **trusts**, nominee and fiduciary accounts the true relationship must be understood. There must be **satisfactory evidence** of any **intermediaries**, Identification includes trustees, settlors/grantors and beneficiaries.	The FI must understand the structure of the company/trust, determine the provider of funds, control over funds, directors. This principle applies regardless of whether the share capital is in registered or bearer form.	**40 Rec. 1996** The existence of the legal entity must be proved (through public registers, legal form, address etc.). FI must take reasonable steps for identification of persons on whose behalf an account is opened. **Review 2002–2003** FATF makes reference to the OECD Report 2001 "Behind the Corporate Veil" and states that the information on the BO of

TOPIC	Basel Committee on Banking Supervision, October 2001 (BCBS)	WOLFSBERG AML PRINCIPLES, May 2002	FATF 40 Recommendations, 1996 and the Public Consultation Paper of review for the FATF 40 Recommendations, May 2002
CORPORATE VEHICLES/TRUSTS	Special care for **bearer shares** (Option: immobilisation of shares e.g. by holding the bearer shares in custody).		corporate vehicles is required for a wide range of purposes. Essential requirements to be met: ■ Adequate, accurate and timely information on the BO (including ongoing changes). ■ Oversight of the systems (special caution with overly complex structures). ■ Access to information for law enforcement and financial regulators. ■ FI and other entities subject to CDD obligations should be able to obtain timely information on BO. ■ Sharing of information on BO with other law enforcement/regulatory authorities or FIUs, both domestically and internationally. *All these requirements are interrelated.* **Trusts:** Aim to enhance the transparency of trusts without limiting the proper use of trusts. Different options*: ■ Upfront disclosure to the authorities of information about all relevant details of trust, trustees, BO and beneficiaries (Option 1a: public register, 1b restricted public access to information) ■ Professional service providers must obtain all relevant information ■ Reliance on investigative powers when illicit activity is suspected. (* The Review Paper is addressed to a wide public and proposes different options, expecting comments from all interested parties.)
WALK-IN-CLIENTS/ THRESHOLD	Not explicitly mentioned, KYC generally required for all customers. Only a general distinction between lower and higher risk customers).	It is left to the bank to determine whether walk-in clients require a higher degree of DD.	**40 Rec. (1996)** No threshold explicitly mentioned, but many FATF member states practise a minimum threshold for identification. **Review 2002–2003** Option to agree to a minimum threshold of Euro 15,000.
NON FACE-TO-FACE CLIENTS	General Risk: Great difficulty in matching the customer with the documentation. ■ Banks should apply customer identification procedures for non-face-to face relationships ■ adequate measures should be compulsory (certification of documents according to face-to-face relationship, independent contact with customer by the bank, cf also *introduced business*).	It is left to the bank to determine whether non face-to-face clients require a higher degree of DD. Bank will address measures to satisfactorily establish the identity of such clients.	**40 Rec. (1996)** Contain only a brief and very general reference to the issue in Rec. 13. **Review 2002–2003** Important topic in the Review Paper. Annex 1 to the Review Paper specifies several options (e.g. face-to-face verification for customers of certain categories, sophisticated online questions, electronic check across several databases).

TOPIC	Basel Committee on Banking Supervision, October 2001 (BCBS)	WOLFSBERG AML PRINCIPLES, May 2002	FATF 40 Recommendations, 1996 and the Public Consultation Paper of review for the FATF 40 Recommendations, May 2002
E-BANKING	BCBS Publication No. 82 Risk Management Principles for e-Banking: ■ Board and management oversight ■ Security controls (appropriate authorisation privileges and authentication measures, logical and physical access control, adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities and data integrity of transactions, records and information). ■ Legal and reputational risk management.	It is left to the bank to determine whether relationships initiated through electronic channels require a higher degree of DD.	**40 Rec. (1996)** Contain only a brief and general reference to the issue in Rec. 13 **Review 2002–2003** Options for handling electronic customer-relationships in Annex 1.
CORRESPONDENT BANKING	Very important part in the BCBS (the FATF text refers to the BCBS, see details in column FATF).	In October 2002 the Wolfsberg Group released new **AML Principles for Correspondent Banking Relationships (CBR Principles).** The following topics are most important: ■ Specified personnel to be responsible for ensuring compliance with the CBR Principles. ■ Risk based Due Diligence to consider the following risks: - CB-Client's domicile. - CB-Client's ownership and management structures (PEPs!) - CB-Client's business and customer base (type of business and type of markets). ■ Requirement of appropriate DD standards of CB-Client (i.e. a regulatory environment that is internationally recongnised). ■ Enhanced DD procedures to CB Clients that present greater risks (PEPs, understanding so-called downstream correspondent clearing-clients, etc.). ■ No shell banks. ■ Updating client files. ■ monitoring and STR.	**40 Rec. 1996** correspondent banking not especially mentioned. **Review 2002–2003** ■ No relationship with shell banks. ■ Correspondent and respondent bank (CB and RB) must document and agree to their respective roles in AML. ■ Information and documentation ab out CB and RB (i.e. info about the respondents ownership, management, major business activities, AML-prevention, other institutions accepted as correspondents, rigour of supervision etc.). ■ Taking measures to deal with risks of "payable-through" accounts (Option: prohibition or full CDD on sub-account holder). ■ Training of staff. ■ Periodic reviews. ■ Special care with NCCTs. ■ Cross reference to BCBS as an option.
VERIFICATION OF IDENTIFICATION (Do the identification documents need to be verified?)	Important part in the BCBS. Verification always required.	Verification not explicitly mentioned but 1.2.1 and 1.2.2 require an identification "to the bank's satisfaction" and "evidence as may be appropriate under the circumstances".	**40 Rec. (1996)** Partially required (esp. for legal entities, Rec. 10). **Review 2002–2003** Verification is an important part and always required.
CUSTOMER PROFILE	Not explicitly mentioned but the existence of a customer profile forms the basis for the distinction between high risk and low risk customers.	The following information must be collected and recorded and forms the basis of a private client **customer profile**: Purpose for opening an account, anticipated account activity, source of wealth and funds, estimated net worth, references to corroborate reputation.	**40 Rec. (1996)** Not explicitly mentioned. **Review 2002–2003** The existence of a customer profile forms the basis for the distinction between high risk and low risk customers.

TOPIC	Basel Committee on Banking Supervision, October 2001 (BCBS)	WOLFSBERG AML PRINCIPLES, May 2002	FATF 40 Recommendations, 1996 and the Public Consultation Paper of review for the FATF 40 Recommendations, May 2002
ONGOING MONITORING	Ongoing monitoring is an essential aspect of effective KYC procedures. Intensified monitoring required for higher risk accounts; Regular reviews of existing clients (e.g. when transaction of significance, customer documentation standards change substantially, change in the way of operating). Ongoing monitoring must be risk sensitive.	Ongoing monitoring is an essential aspect of effective KYC with WB. Sufficient monitoring program must be established. Private Banker must be especially aware of unusual or suspicious activities. Automated systems are suggested to support ongoing monitoring.	Ongoing monitoring is an essential aspect of effective KYC with the FATF (1996 and the Review Paper).
DOCUMENTATION	Documentation required. Records must remain up-to-date.	Documentation required. Records must remain up-to-date.	Documentation required. Records must remain up-to-date.
SUSPICIOUS ACTIVITY REPORTING (SAR)	Not the focus of the BCBS.	Not emphasised, instead focus is on the identification of unusual or suspicious activities. Reporting is only mentioned as a follow-up procedure of unusual or suspicious activities.	**40 Rec. (1996)** Obligation to report, if FI funds stem from a criminal activity (Rec. 15). **Review 2002–2003** Option to allow an indirect reporting system as sufficient (instead of a direct reporting system). Option to extend "suspect" to "suspect or have reasonable grounds to suspect" (making the text objective as well as subjective).
DELEGATION	No reference.	No reference.	**40 Rec. (1996)** No reference. **Review 2002–2003** Identification and verification obligations can be outsourced (e.g. to agents). However, FATF leaves the further examination to the common business practices (Margin Note 105).
INTRODUCED BUSINESS	Bank can rely on introducer under the following conditions: ■ Ultimate responsibility of the recipient bank on KYC and customers business (special caution when introducer subject to lower standards or unwilling to share copies of DD Documentation). ■ Assessment whether introducer is "fit and proper" and is exercising the necessary DD in accordance with the BCBS standard. ■ Criteria for reliability of introducer are: - same CDD standards as in BCBS Standard, - bank must be satisfied with CDD system used by the introducer, - verification of CDD made by introducer must be possible at any stage, - identification data must be submitted to bank (i.e. introducer must not be bound to professional secrecy). ■ Periodic reviews of introducer.	Distinction between introducing intermediary, managing intermediary (professional asset manager) and agent intermediary. **Introducing intermediary:** ■ Is only introducing clients to the bank. ■ Is not the account holder, BO or signatory. ■ If bank relies on DD conducted by the intermediary, the bank must be satisfied with the DD procedures. ■ Reputation and integrity must be satisfactory. **Managing intermediary:** ■ Acting on behalf of one or several clients. ■ May be the account holder (but not the BO).	**40 Rec. (1996)** No reference. **Review 2002–2003** Reliance on third parties: ■ if a FI relies on third party identification or verification of identity the ultimate responsibility always with the FI. ■ All relevant data must be submitted to the FI immediately (information must be available for review by the supervisor). ■ Third party must be subject to full range of AML requirements set out by FATF (i.e. customer identification and verification practices) and must be regulated. ■ FI must check regularly the reliability of the third party and must enter into a written agreement.

TOPIC	Basel Committee on Banking Supervision, October 2001 (BCBS)	WOLFSBERG AML PRINCIPLES, May 2002	FATF 40 Recommendations, 1996 and the Public Consultation Paper of review for the FATF 40 Recommendations, May 2002
INTRODUCED BUSINESS		■ May act on behalf of a particular client or on a pooled basis (fund or portfolio manager). ■ Reputation and integrity must be satisfactory. ■ Bank should know about the relationship between intermediary and BO. ■ Intermediary must be regulated. **Agent intermediary:** ■ Signatory authority but does not act on a professional basis. ■ Not account holder or BO of an account. ■ Usually not DD on this type of intermediary.	*FATF does not intend to put detailed issues into the Recommendations, but only intends to add a single sentence and make cross references to guidelines and best practices.*
PROFESSIONAL INTERMEDIARIES	In general: if a pooled account is held by a professional intermediary the BO must be identified. But, if the PI is subject to the same regulatory and ML legislation and procedures and to the same DD standards, the banks do not have to look through to the BO. National supervisory guidance should clearly set out those circumstances. If a PI is bound by a professional secrecy (lawyers) or has lower standards, the bank should not permit an account to be opened.	Cf. introduced business.	**40 Rec. (1996)** No reference. **Review 2002–2003** Cf. introduced business.
PROFESSIONAL SECRECY	Intermediaries bound to professional secrecy should **not** be **permitted** to open an account (e.g. lawyers).	No reference.	**40 Rec. (1996)** Not explicitly mentioned in the 40 Rec. but in the typologies reports. **Review 2002–2003** It is proposed that the FATF framework should cover independent legal professionals. Several options are to be considered, such as ■ covering **lawyers** and independent legal professionals in all their activities (or **notaries** in all countries). ■ covering the above only when acting as financial intermediaries. ■ covering the above when they are involved in execution of financial, property, corporate or fiduciary business. ■ the above should be subject to the same CDD and Suspicious Transaction Reporting obligation as FI, as well as to regulation and supervision (either SRO or state supervision).
RISK CATEGORIES	Risk categories are an essential precondition for the implementation of the RBA.	Banks are required to define categories of persons whose circumstances warrant an additional diligence. Distinction between higher and lower risk customer.	**40 Rec. (1996)** No reference. **Review 2002–2003** Distinction in higher and lower risk customer (or transactions) is essential with the FATF.

TOPIC	Basel Committee on Banking Supervision, October 2001 (BCBS)	WOLFSBERG AML PRINCIPLES, May 2002	FATF 40 Recommendations, 1996 and the Public Consultation Paper of review for the FATF 40 Recommendations, May 2002
RISK BASED APPROACH (RBA)	Supports the application of the RBA. Reputational, operational, legal and concentration risk must be assessed.	Supports the application of the RBA.	Supports the application of the RBA.
PEPs	Considered as a high risk category. Banks should gather sufficient information, check the source of funds, involvement of senior management required, ongoing monitoring essential.	Considered as a high risk category requiring additional diligence. PEPs and their family and close associates should be treated with heightened scrutiny, especially PEPs from countries without adequate AML standards, NCCT need enhanced treatment. Asking clients about their political function should be part of the standardised account opening procedure. Approval of senior management required.	FATF has various concerns with respect to PEPS but refers in the options to the BCBS. (One other option would be to include PEPs in a new CDD Recommendation, in which other topics would be dealt, such as correspondent banking, reliance on third parties etc.).
PRIVATE BANKING	Private Banking: Approval of person of seniority other than private banking manager and if higher confidentiality established banks must ensure same scrutiny and access for compliance officers and auditors must be given.	The WB AML Principles refer to private banking relationships only.	**40 Rec. (1996)** No reference. **Review 2002–2003** Not explicitly mentioned, but the list of high risk customers or transactions deal mostly with the profile for private banking clients.

List of abbreviations

ABS Guidelines	Guidelines on the Prevention of the Misuse of the Singapore Banking System for Money Laundering Purposes, dated September 2001, issued by the Association of Banks in Singapore ("ABS")
BO	Beneficial Owner
BSA	Bank Secrecy Act
C	Customer
CB	Correspondent Banking
CDB 03	Code of Conduct, latest edition effective as of 1 July 2003
CDD	Customer Due Diligence
CIP	Customer Identification Programs
DD	Due Diligence
EB	Electronic Banking
FI	Financial Institution
FTF	Face-To-Face
ID	Identification
JMLSG	Joint Money Laundering Steering Group
KYC	Know Your Customer
ML Ordinance	Ordinance of the Swiss Federal Banking Commission Concerning the Prevention of Money Laundering, effective as of 1 July 2003
MLA	Money Laundering Act
MAS	Monetary Authority of Singapore
NFTF	Non Face-To-Face
No reference	Study contains no reference to the topic
PA	Patriot Act
PB	Private Banking
PEP	Politically Exposed Person
PI	Professional Intermediary/-ies
RBA	Risk Based Approach
SAR	Suspicious Activity Report/-ing
ST	Suspicious Transaction
TO	Terrorist Organisation
TF	Terrorist Financing

Bibliography

Garland, David

The limits of the sovereign state, strategies of crime control in contemporary society, The British Journal of Criminology 1996, p. 445 et seq.

Kilchling, Michael

Die Praxis der Gewinnabschöpfung in Europa, in: Kriminologische Forschungsberichte aus dem Max-Planck-Institut für ausländisches und internationales Strafrecht, Band 99, Freiburg i.Br. 2002.

Levi, Michael / Gilmore William

Terrorist Finance, Money Laundering and the Rise and Rise of Mutual Evaluation: A New Paradigm for Crime Control? in: Financing Terrorism (Ed. Mark Pieth), Kluwer Academic Publishers 2002, p. 87 et seq.

Pieth, Mark

The Prevention of Money Laundering: A comparative Analysis, European Journal of Crime, Criminal Law and Criminal Justice 1998.

The Harmonization of Law Against Economic Crime, in: EJLR 1998/1999, p. 527 et seq.

Staatliche Intervention und Selbstregulierung der Wirtschaft, in: Festschrift für Lüderssen, Baden-Baden 2002, p. 317 et seq. (Festschrift für Lüderssen)

Sansonetti, Riccardo

The Mutual Evaluation Process: A Methodology of Increasing Importance at International Level, in: Journal of
Financial Crime, Vol. 7, No. 3, 2000, p. 222 et seq.

Die Problematik der Offshore-Finanzzentren und die Position der Schweiz, in: Die Volkswirtschaft – Das Magazin für Wirtschaftspolitik 2/2001, p. 40 et seq.

Savona, Ernesto

Obstacles in Company Law to Anti-Money Laundering International Co-operation in European Union Member States, in: Financing Terrorism (Ed. Mark Pieth), Kluwer Academic Publishers 2002, p. 57 et seq..

Wymeersch, Eddy

Study of the regulation and its implementation, in the EU Member states, that obstruct international anti-money laundering international co-operation, in: Transcrime, Transparency and Money Laundering, (October 2001);

Winer, Jonathan M.

Globalization, Terrorist Finance, and Global Conflict – Time for a White List?, in: Financing Terrorism (Ed. Mark Pieth), Kluwer Academic Publishers 2002, p. 5 et seq.