Globalization, Terrorist Finance, and Global Conflict: Time for a White List?

Jonathan M. Winer*

I. 11 September 2001: Global Financial Transparency Under Construction

When the terrorists trained by Osama bin Laden destroyed the two World Trade Center towers, their actions revealed both the globalization of terrorist finance, and the potentially Herculean task facing governments seeking to combat both it and other serious trans-border problems involving flows of money from illicit sources or for illicit purposes. Relying on a mere 500,000 USD in total expenditures, nineteen terrorists were able to enter the United States repeatedly, train as commercial pilots, engage in intercontinental air travel, rent cars, establish personal bank accounts, obtain ATM cards, and generally live adequately funded lives in the months prior to the attack. After 11 September, some of the funds involved were traced to an account in Dubai, a country that houses not only its own banks, but major US and European banks, banks from throughout the Islamic world, purely Islamic banks, alternative or underground remittance systems (hawalas), gold dealers, and myriad financial institutions handling transactions to such States as Iran and Iraq.

While little had been done to implement the standards at the time, Dubai was actually one of the very few countries in the Middle East (the others being Cyprus and Israel) to have even basic money laundering legislation in place. In theory, since the previous year, financial institutions in Dubai had been prohibited from taking anonymous funds for anonymous accounts, which previously had been lawful. By contrast, if one wanted to place funds for a terrorist from Saudi Arabia, for example, or from Bahrain, Yemen, Malaysia, Indonesia, the People's Republic of China, the

---

* The author was US Deputy Assistant Secretary of State for International Law Enforcement from 1994 through 1999. He currently practices international financial services law at the firm of Alston & Bird LLP in Washington, DC and can be contacted at jwiner@alston.com. An earlier version of this paper was undertaken in late 2001 and early 2002 with the support of the Norwegian FAFO Institute in Oslo, Norway.

M. Pieth (Ed.), Financing Terrorism, 5–40.

Philippines, Nigeria, or Somalia, to name only a few, opportunities for anonymity would be wide-open. In these countries, there were effectively no limits on the anonymous placement of money, either in law or in practice, and indeed several of them retained a legacy of large numbers of anonymous accounts that could be freely traded as needed to practically anyone.

Sources of funds for terrorism were also little constrained. For Islamic terrorists, vast sums were available to those carrying out charitable work, including militant resistance, in Islamic outposts under siege – such as Bosnia, Kosovo, Kashmir, and Chechnya – donated by wealthy Gulf State Muslims giving zakir. Further funding was made available by siphoning off donations for more ordinary charitable work in many other jurisdictions within Islamic communities. These funds merely added to the seed money available on an ongoing basis from the proceeds of narcotics. Alternatively, terrorists have had numerous opportunities to generate revenues through fraudulent conversion of social benefits, migrant smuggling, document fraud, stealing cars, gun-running, or even working for the money. Thus, money, the life-blood of all kinds of organized crime, and regardless of its involvement in terrorist deposits and withdrawals has coursed rather freely through the veins of the global financial infrastructure.

Long before 11 September, other forms of financial scandal had demonstrated the ease with which criminals, drug traffickers, illicit combatants, guerrillas, and other persons and entities engaged in socially condemned behaviour have been able to launder their money. And repeatedly, governments, regulators, law enforcement agencies, and the most important and prestigious international organizations have found themselves unable to trace illicit transactions after something goes radically wrong.

Thus, terrorist finance can be seen from this perspective as a subset of a larger problem, that of non-transparent movements of money in a system to which much of the world has easy access. Financial non-transparency has facilitated not only terrorism, but also many of the world's more significant social ills, including civil war and civic instability. For example, the laundering of the proceeds of crime is a necessary means to carry out the trade in diamonds that has fuelled civil conflict in Liberia, Angola and Sierra Leone, together with their accompanying arms deals and payoffs. The narcotics trade has long been understood as a massive generator of illicit money to be laundered, as well as a generator of corruption and weakened governance. Drug trafficking is also closely associated with conflict, and one of the enduring factors in such conflict is the fact that drug funds sustain combatants in civil wars. It is no accident that each of the three countries which produce most of the world's opium and coca crops – Afghanistan, Burma, and Colombia – have ongoing insurrections fuelled by drug money, in which terrorist acts (or their equivalents) have become a common element of daily life.

The global attention focused on terrorism and terrorist finance as a result of the 11 September attacks on the United States provides a fresh vantage point on what has become an increasingly longstanding, significant problem. As an increasing number of significant global problems became linked to illicit finance, money

laundering was recognized in the 1990s as a global problem requiring a global response. Prior to 11 September, this response included new international instruments, such as the 2000 United Nations Convention to Combat Transnational Organized Crime and the Second Money Laundering Directive, issued by the European Union in late 2001. It has also included the rapid movement of 'name and shame' sanction programmes. Most prominent among these has been the Financial Action Task Force (FATF) against 'non-co-operative countries and territories'. In the first two years that the FATF threatened to limit market access to jurisdictions not meeting international standards, most of the nearly twenty targeted jurisdictions enacted new anti-money laundering laws. A similar exercise against 'unfair tax competition' undertaken by the Organization for Economic Cooperation and Development (OECD) is having a similar impact on ring-fencing, the strategy by which jurisdictions offer non-residents unregulated financial services, which they deny to their own citizens.

Major self-regulatory organizations, such as the Basel Committee for Banking Supervision (BGBS), the International Organization of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors (IAIS) also focused on extending standards for international regulation to cover transparency issues.[1] The new standards were designed to respond to the major failures of existing financial regulation to provide protection against illegal activities. Each organization focused on major gaps in the international regulatory system that translated into injuries to domestic supervision and enforcement. These gaps included:

- Fragmented supervision within countries by sector and among countries by national jurisdiction.
- Exploitation of differences in national provisions for regulatory arbitrage to circumvent more stringent national laws and international standards.
- Secrecy laws which impede the sharing of information among countries and between regulators and law enforcement.
- Inadequate attention to electronic payments in existing anti-money laundering supervision and enforcement, including 'know your customer' rules that focus on currency, even as the world's financial services businesses rapidly continue their move into e-money.
- The lack of international standards governing key mechanisms used in transnational financial transactions, such as international business companies (IBCs), offshore trusts, offshore insurance and reinsurance companies, and offshore funding vehicles, including but not limited to hedge funds.

---

[1] *See*, e.g., Statement of the G-7, 18 June 1999; 'Strengthening the International Financial Architecture', Report of the G7 Finance Ministers, 18–20 June 1999; 'Financial Havens, Banking Secrecy and Money-Laundering', UN ODCCP, New York, May 1998; and numerous recent analytic documents of the Basel Committee available on the website of the Bureau of International Settlements (BIS).

- Minimal due diligence by company formation agents, attorneys, and financial institutions in the process of incorporating and licensing of new financial institutions and shell companies and trusts owned by their affiliates.

In response, there has been a convergence in the standards of protection in many countries against various simultaneous threats. In essence, the standards have begun to require a form of 'know your customer' at both the front end and the back end of any transaction. At the front end, bankers and other financial facilitators are now required to know with whom they are dealing, and at some level, what their customers have been doing with their money. At the back end, those permitting withdrawals of funds need to know not only who has been getting the money but also where it came from. That way, should something go wrong, it should be possible to trace the funds.

Despite these efforts, the globalization of money makes tracing increasingly more difficult.

Thus, the need to establish uniform standards, end bank secrecy, create mechanisms for the exchange of information between national regulators and law enforcement organizations with their counterparts, and the decision to 'name and shame' jurisdictions that failed to adopt and live by the new rules. In 1989, when the FATF was created, there was some scepticism about the ability of even OECD countries to agree on common standards, let alone to live by them. A decade later, when the FATF's non-co-operative countries and territories initiative began, common standards became comprehensive, and the consensus existed that they should be made universal. Thus, by 11 September, the name and shame exercises were well on the way to universality. Over time, the existing international initiatives in response to these problems began to create a new global code articulating new international standards for transparency. And yet, these initiatives failed to do much to prevent the September terrorists from carrying out their plans.

One could argue that these regimes are too new and incomplete to have had an impact, especially in a world where the proceeds of the world's largest extractive industry, oil, remained largely opaque despite all of the transparency initiatives. In this view, objectives are long-term and the belated response to the globalization of the financial infrastructure cannot be expected to fix long-standing problems overnight, especially in such regions as the Middle East, which only began to adopt the regulatory standards of more established international financial services centres.

However, it is also possible that the basic idea of a universal standard for all governments, given our global diversity, is inherently flawed. Each of the new initiatives has been based on the promise that national financial service regulators have the capacity to determine whether their own 'local' institutions meet the standards or not. Under the principle of consolidated supervision, the home-country regulator of any international financial institution is solely responsible for exercising oversight over the global operations of that institution. Over the past ten years, the principle of consolidated supervision has proven helpful but far from infallible in protecting safety and soundness by requiring multi-jurisdictional financial institu-

tions to take at least their home regulators very seriously. In turn, these home regulators are increasingly subject to a common set of standards, such as those established by the Basel Group of Bank Supervisors (Basel Group). Over time, these standards have come to promote global financial stability by promoting good practices for banks in their lending and investment practices. However, the same system has to date demonstrably failed to do much to protect the world from money laundering or terrorist finance.

II. The Capacity Problem

Can governments that stop at borders regulate financial activity that crosses borders at the speed of light amid billions of electronic ones and noughts? Even if one does not consider the special problems posed by terrorist finance and the inadequacy of financial transparency regimes in the Middle East, there is mounting evidence to justify questioning whether global banks, operating transnationally to move money instantaneously across national borders, can be readily regulated or supervised by any one country. While such financial institutions may have their headquarters nominally based in a single country – typically one of the G–7 countries, the EU, or Switzerland – they generate profits and carry out activities at a global level involving dozens of UN Member States. As a result, they are for many purposes beyond the capacity of any single state to police. The current 'name and shame' exercises have had the salutary effect of forcing some of the world's least-adequately regulated jurisdictions to abandon traditional notions of bank secrecy, and to begin insisting that their financial institutions carry out due diligence and know their customers. But these exercises have not and cannot create any capacity at a national level to assess the meaning and integrity of cross-border financial transactions. It is not reasonable to expect a small jurisdiction that houses a subsidiary of a major international financial institution to fully understand the cross-border transactions engaged in by the subsidiary, let alone by its affiliates or far-away parent. In practice, even the most sophisticated and best regulated financial centres, including those of the G–7, European Union, and Switzerland, are similarly incapable of exercising adequate oversight over the global enterprises they license.

In recent years, the proposed solution has been a mixture of public sector regulation and private sector self-regulation. Self-regulation has been advocated as a means by which private institutions subject to market forces will, as a matter of good business, avoid transactions that are exposed on that institution or its reputation to undue risk. However, it is not clear that this approach has been effective. Indeed, the combination of both government regulation and self-regulation has not to date effectively discouraged abuse of international financial institutions by drug traffickers, terrorists, major financial criminals, corrupt officials, arms smugglers, or sanctioned regimes, not to mention those engaged in

How Can Sound Customer Due Diligence Rules Help Prevent the Misuse of Financial Institutions in the Financing of Terrorism?

Charles Freeland*

When the author first joined the Basel Committee Secretariat in 1978, the idea that bank supervisors had a role to play in the prevention of money-laundering would have been greeted with astonishment. Some ten years later, when Basel first discussed the topic in earnest, there was still a body of opinion that this was a matter for law enforcement and supervisors should stick to the core tasks they were charged with. Nonetheless, the Basel Committee (BCBS) agreed, principally at the insistence of the United States, to issue a statement alerting banks to their ethical responsibilities in the prevention of the criminal use of the banking system. At that time the principal concern was to make it more difficult and costly for drug gangs to launder the proceeds of their crimes. That statement,[1] relatively short by today's standards, laid down four principles that banks should follow:

- Identify their customers
- Refuse suspicious transactions
- Co-operate with law-enforcement agencies
- Train their staff and introduce compliance procedures.

This statement exerted quite wide influence at the national level in the major industrialized countries and was additionally one of the triggers for the formation of the Financial Action Task Force (FATF). With the creation of the FATF, the BCBS took the view that the baton could be passed over to a body with the necessary wider competencies. Although invited to participate in the FATF, the BCBS declined on the grounds that its views could be adequately represented by the individual bank supervisors who became members.

But times change. In 2000, one of the BCBS's specialist task forces, the working

---

* Deputy Secretary General, Basel Committee on Banking Supervision. Charles Freeland is writing here in his personal capacity. The views expressed in this article do not necessarily represent the views of the Basel Committee or the Bank for International Settlements.

[1] *The prevention of the criminal use of the banking system* (1988).

M. Pieth (Ed.), Financing Terrorism, 41–48.

group on cross-border banking, decided to revert to the issue principally as a result of a series of scandals involving banks' relationships with corrupt dictators such as Abacha and Salinas (now termed 'Politically Exposed Persons' (PEPs)) as well as with the Russian Mafia. The working group on cross-border banking is something of a hybrid animal – it was originally created as a joint working group of the BCBS and the Offshore Group of Banking Supervisors (OGBS) to discuss issues relating to the implementation of the Basel Concordats that govern the responsibilities of bank supervisors in their supervision of international banking groups and their cross-border establishments. As a result, it is co-chaired by the OGBS chairman, Colin Powell, and the author. Its deliberations focus mainly on practical issues such as exchanges of supervisory information, cross-border inspection rights and corporate structures that impede banking supervision. A key product of this work, which will be reconsidered at the end of this article, is the creation of a platform for information exchanges between bank supervisors that is designed to improve supervisory coordination and enable home-country supervisors to exercise consolidated supervision. Such information exchanges have always been impeded by bank secrecy legislation and practices that are regarded by some private banking centres as a competitive necessity in order to prevent information on customer accounts in cross-border entities from being passed to home-country tax authorities. Hence, the supervisory Concordats developed by the Basel Committee have had to balance the need for adequate gateways with the need for adequate protection of information received.

The reason why the cross-border group became concerned about the risks to banks in this area was not only its concern about PEPs (initially called 'potentates'). A survey of know-your-customer (KYC) standards around the world revealed that, despite the FATF's successful initiatives in its member countries, many countries still had no KYC standards at all. The BCBS has the ability to set rules for banks and bank supervisors that, through its influence as a standard-setter and with support from the IMF and World Bank, can have a much broader reach than the FATF. In addition, the FATF's focus is on criminal activity, in its early years especially those activities involved in laundering the proceeds of drug sales, whereas the BCBS is concerned with the risks to banks from a much wider range of unsuitable customers – the PEPs issue is a case in point. Moreover, the BCBS saw a need to respond to the call by the G-7 to strengthen defences against abuse of the financial sector by producing a benchmark for Customer Due Diligence (CDD) standards for banks, as well as a need to act on requests from many emerging market supervisors for guidance in this area.

The BCBS's working group on cross-border banking's expertise in offshore centres and international banking meant that it possessed the qualifications for identifying the risks being posed to international financial institutions. Several of its members are FATF participants. The BCBS therefore agreed with the group's proposals that it address KYC rules for banks. This title was subsequently amended to Customer Due Diligence (CDD) standards to reflect the wider and continuous duties of the banker in protecting a bank's good name.

The working group was producing a draft set of standards at exactly the time that

the Wolfsberg Group's first document was being prepared. In each case, the principal trigger was the Abacha affair. The BCBS's consultative paper[2] did not address money-laundering or suspicious transaction reporting directly. Rather its focus was on risk management for banks in their customer relationships. The paper focused on four specific risks; reputation risk, legal risk, operational risk and concentration risk (essentially liquidity/funding risk). Plainly, the most sensitive of these is reputation risk. A key distinction was drawn between initial identification of each new customer and ongoing monitoring of existing account activity.

The reaction of the supervisory community to the BCBS's draft was wholly supportive, including enthusiasm from some countries that one would not have put high on the list of those interested in probity. The FATF was also supportive and the Wolfsberg Group provided constructive comments. But some banks and banking associations were less enthusiastic. They raised two principal concerns that we sought to address in the final version of the paper that was issued in October 2001. One was the regulatory burden issue – and that is a very justifiable concern. We tried to respond to that by introducing a risk-based approach – identifying higher-risk customers or customer activities that merit heightened due diligence, and reducing the burden of monitoring the identities and activities of 'ordinary' retail clients. Indeed, the paper makes clear that while customer identification procedures are needed, they should not be so restrictive as to deny banking services to people who are financially or socially disadvantaged – and the same for ongoing monitoring. A second concern related to the clause requiring banks to backdate their customer identification procedures to existing clients. This could be very burdensome for banks serving small retail customers. Although there is still in the final version a requirement to undertake regular reviews of existing records and to monitor the activities of long-standing clients, there is now no obligation for banks to demand customer identity documentation from existing customers.

So what has all this to do with the fight against terrorist financing? Well, first, the bank needs to know who its customers are if it is to be able to respond to requests from law-enforcement or intelligence authorities concerning accounts in the names of known terrorists or terrorist organizations. By definition, however, terrorists may be reluctant (and that reluctance is likely to be greater in the future) to open an account under their true names. They will thus try to hide behind anonymous accounts or 'fronts' making use of trusts, charities, nominees, corporate vehicles, profession intermediaries, and so on. The CDD paper gives clear guidance to banks on how to prevent such fronts from being used by criminals, including of course terrorists. This is a complex area in practice, but the principle itself is clear: the bank must make every effort to establish the beneficial owner(s) of all accounts and persons who conduct regular business with it.

---

[2] *Customer Due Diligence for Banks*, January 2001. Although the document was targeted at banks, it expresses the view that similar guidance needs to be developed for all non-bank financial institutions.

The key to preventing terrorists from using banks has to be in the initial customer identification process. Once an account is open, it will rarely be feasible for a bank to identify unusual account activity by a terrorist. The patterns of account activity by the Al-Qaeda perpetrators of the 11 September tragedy are by no means abnormal for a person with an irregular source of income such as a consultant, or a student with occasional parental support. Account profiling is therefore unlikely to identify a terrorist customer. What would of course help would be a tip-off from another source, maybe an intelligence source, or the observation by an alert staff member that the customer's behaviour is suspicious. Another pointer could be that the origin or destination of funds is a terrorist organization. However, one cannot expect banks to monitor every transaction of what would likely be classified as a low-risk customer. What one can do, and what the BCBS's CDD paper does, is to insist that banks maintain account and transaction records for at least five years so that the audit trail can be followed and the origins or source of funds followed if required.

The BCBS paper lays down clear guidelines for customer acceptance and customer identification procedures to be followed by banks in the opening of new customer accounts. It advises individual supervisors to establish strict standards for the documentation that should be required – and prohibits the use of anonymous accounts. It does not specifically list the categories of documents that banks should demand to see. There was an annex attached to the January consultative paper that gave examples of the types of documentation that could be admitted. However, the working group excluded this from the final October version because it felt that more attention was needed to the issue. It is now planning to provide more detailed guidance on customer identification procedures in due course, and to use that opportunity to update the October paper with any further guidance on CDD that has emerged from consultations in other bodies. To take one example, the FATF and the Wolfsberg Group have made certain proposals for the completion of the field for the originator's name in the transmission of wire transfers. The BCBS will probably want to establish a best practice guideline for that issue in due course.

Nobody should be under any illusions that conducting customer due diligence is a simple task – it is one that is full of contradictions. The culture of banking is engrained in the desire to attract customers and profit from providing banking services. As with retailers selling products that are not suitable for all, there needs to be a highly-developed social conscience to prevent banking services falling into the wrong hands. Ex post, it can be relatively easy to judge that a customer should not have been accepted – ex ante, with the pressure on to welcome and even reward new customers, the task is more challenging. There are behavioural differences to respect, for example, in relation to well-heeled customers from other countries. The compliance officer or risk manager in charge of customer due diligence will be in constant conflict with the incentives provided to customer service units dedicated to personal, private or offshore banking. There may also be conflicts of culture with regard to what may or may not be regarded as acceptable behaviour by foreign customers. This may go way beyond the bank – for example the UK is currently grappling with the diplomatic ramifications of the freezing of an account linked to a

Qatari Minister who received 'facilitation payments' for a UK defence deal. The UK's Treasury and Home Offices are apparently in favour of the freeze, while the Defence and Foreign Ministers oppose it. One can only sympathize with a bank that gets involved in such a tug of war.

Fortunately, conflicts of this kind are not likely to arise with regard to terrorist financing. However, there are other aspects that complicate the issue for the financial sector. One of the difficulties in providing guidance to banks in the fight against terrorism is to define what is a terrorist or a terrorist organization. There is often a thin line between terrorists and freedom fighters and a good number of current and recent Heads of State were once regarded as terrorists. The EU definition is more subtle 'persons who finance, plan, facilitate or commit terrorist acts', and it goes on to define a terrorist act. Nonetheless, it is a difficult issue on which the private sector needs guidance from the authorities, and it is not guidance that the supervisors can easily provide. Rather, the financial sector needs to receive information from police and intelligence as to the terrorists and terrorist organizations on the 'black list'. This is even more true in the case of charities and foundations. Many innocent-sounding organizations that may raise money from legitimate sympathizers who believe they are contributing to a humanitarian cause have, in the past, been channelling at least a portion of the funds they have raised to terrorist uses.

Much has been made by the media and by professional writers of the fact that terrorism is different from money-laundering because it is the **use** of the funds that is criminal not their **source**. However, it may be wrong to place too much emphasis on this factor to explain why banks are unable to identify customers engaged in terrorism. There has not, to the author's knowledge, been a significant terrorist organization to date that has funded itself wholly from legitimate means. Al-Qaeda has been heavily involved in the marketing of drugs as well as other lesser crimes such as credit card fraud. Terrorist organizations are certainly not beyond robberies, kidnapping, extortion, and so on as a means of financing their illegal activities. Building and maintaining an effective terrorist organization costs a great deal of money – in the case of Al-Qaeda hundreds of millions. Hence, successfully denying all criminals access to the financial system will hit the terrorists too. What may be more challenging will be the identification of charities and other fund-raising organizations that support terrorism. Many of the contributors to what are usually set up with innocent sounding titles may not be aware that their money is being channelled into a terrorist organization.

One concern that arises in the present hunt for Al-Qaeda money is that the terrorists will turn increasingly to parallel underground banking systems. Attention has been focused on the Hawala system – but it is by no means the only one for money transmission. Western Union type transfer systems, travellers cheques, even credit cards can be an effective means of financing individual terrorists if not whole terrorist cells. Much has also been made of the need to crack down on correspondent banking relations. Effectively, a respondent bank is relying on its correspondent to have conducted due diligence of each of its customers, because there is no way the respondent bank can monitor the probity of all transactions originating from sources

Financing of Terrorism – A Predicate Offence to Money Laundering?

Armand Kersten

1. Introduction

On 30 October 2001, the Financial Action Task Force on Money Laundering (FATF) agreed to a set of Special Recommendations on Terrorist Financing.[1] Recommendation II provides:

> 'Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. *Countries should ensure that such offences are designated as money laundering predicate offences.*' (emphasis added, AJK)

These Special Recommendations were agreed upon at a FATF 'extraordinary Plenary', at which the FATF extended its mission beyond money laundering.[2]

The 11 September 2001 attacks on America triggered drastic legislation aimed at suppressing the financing of terrorism,[3] appearing to depart from the legal apparatus, classically used in the fight against money laundering. For instance, the significant part of the USA PATRIOT Act package is the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. In the Act, the American Congress finds that money laundering permits transnational criminal enterprises to conduct and expand their operations to the detriment and safety of American citizens, and that *money launderers subvert legitimate financial mechanisms and banking relationships by using them as protective covering for the movement of criminal proceeds and the financing of crime and terrorism.*

By making a brief *tour d'horizon* of relevant source materials from international (institutional) organizations, this paper shall address whether, from a methodolo-

---

[1] FATF news release of 31 October 2001, FATF cracks down on Terrorist Financing (available on the web at <http://www1.oecd.org/fatf/TerFinance_en.htm>).

[2] See the news release mentioned in ibid.

[3] Two of the highest profile laws in this category being the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ('the USA PATRIOT ACT') and the UK Anti-Terrorism, Crime and Security Act 2001.

M. Pieth (Ed.), Financing Terrorism, 49–56.

gical perspective, it makes sense to legislate to suppress financing of terrorism on the basis of analogies with money laundering.

2. Money laundering

Whilst the *United Nations Convention against illicit traffic in narcotic drugs and psychotropic substances* of 19 December 1988 ('the Vienna Convention') created momentum for the attention to money laundering as a global phenomenon,[4] it only required the prohibition of the 'laundering' of *drug proceeds*.[5] Note that the FATF, in its initial 40 Recommendations of 1990[6] took the 'definition' of money laundering from the Vienna Convention.

The Council of Europe[7] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 8 November 1990[8] (the Strasbourg Convention), takes this a step further, by giving its Article 6 the title: 'Laundering offences'. Whilst repeating constituent elements already contained in the Vienna Convention, it widens the circle of 'predicate offences' beyond drug trafficking. In so far as is relevant for the purposes of this article, it provides that the parties must establish as offences under their domestic laws:

a. the conversion or transfer of property, knowing that such property is *proceeds* for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the *predicate offence* to evade the legal consequences of his actions;
b. the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to or ownership of property, knowing that such property is proceeds and subject to its constitutional principles and the basic concepts of its legal system;
c. the acquisition, possession or use of property, knowing, at the time of receipt, that such property was proceeds. (emphasis added)

---

[4] The term 'money laundering' as such seems to have been introduced in the US Money Laundering Control Act of 1986.

[5] It is noted that the Vienna Convention does not explicitly refer to (the term) money laundering.

[6] Later in this article, it will be seen that the 1996 revision aimed at widening the scope.

[7] The Council of Europe should not be mistaken with the European Council. The Council of Europe is an international institutional organization, whereas the European Council is an organ of the European Union.

[8] Available on the web at < http://conventions.coe.int/treaty/en/Treaties/Html/141.htm >.

The Strasbourg Convention defines 'proceeds' as: *any economic advantage from criminal offences.*[9] It goes on to define 'predicate offence' as: *any criminal offence as a result of which proceeds were generated that may become the subject of an offence as defined in the 'laundering article'.*[10] This yields an entirely open-ended range of predicate offences, hinging on the definition of 'proceeds' as *any economic advantage from criminal offences.* Perhaps the only limitation is hidden in the fact that it is left to the Member States to incorporate the convention's requirements in their domestic criminal laws, which leaves them discretion to draw the circle themselves.

The Commission of the European Communities labelled the methodology of the Strasbourg Convention: '*an approach to combating the laundering of the proceeds of a wider range of criminal offences than required by the Vienna Convention*' (emphasis added).[11]

I now turn to the European Union (and the European Communities) itself. The Council of the European Communities Directive of 10 June 1991 on prevention of the financial system for the purpose of money laundering[12] provides:

> 'Whereas for the purposes of this Directive the definition of money laundering is taken from that adopted in the Vienna Convention; whereas, however, since money laundering occurs not only in relation to the proceeds of drug-related offences but also in relation to the proceeds of other criminal activities (such as organized crime and *terrorism*), the Member States should, within the meaning of their legislation, extend the effects of the Directive to include *the proceeds of such activities*, to the extent that they are likely to result in laundering operations justifying sanctions on that basis.' (emphasis added)

The 1991 Convention thus envisages and recognizes that terrorism is a criminal activity potentially resulting in proceeds in relation to which money laundering may occur. From a logical perspective, however, it seems that this approach presumes the criminal activity preceding the laundering of the proceeds.

In 1996, the FATF strengthened its 4th Recommendation to state that 'each country should extend the offence of drug money laundering to one based on serious offences', done so as to extend the ambit of the predicate offences beyond that of the Vienna Convention.

---

[9] Article 1, sub a.

[10] Article 1, sub e.

[11] Commission of the European Communities, Proposal for a European Parliament and Council Directive, amending Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, Brussels, 14 July 1999, *COM* (1999) 352 final, explanatory memorandum.

[12] OJ 1991 L 166, p 77 *et seq.*

In 1998, under the auspices of the UN Office for Drug Control and Crime Prevention,[13] the report *Financial Havens, Banking Secrecy and Money Laundering*[14] was published. Under the header 'issues for consideration', this report addresses 'predicate offences'[15]:

> 'The time may have come to end the artificial division of criminal money into categories depending on the nature of the crime. ... One possible approach would be to have member countries agree that any funds that are derived through criminal activity are funds that can give rise to a charge of money-laundering.'

From the context of the report, it can be inferred that the term 'artificial division' is used to point to distinctions sometimes made between *criminal* tax offences and tax offences classified otherwise.

On 9 December 1999 the General Assembly of the UN adopted the International Convention for the Suppression of the Financing of Terrorism.[16] Article 2 provides, in so far as is relevant here:

> '1 Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
> [...]
> (b) Any other act [subparagraph (a) refers to acts constituting offences under a list of treaties] intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do so or to abstain from doing any act.
> [...]
> 3. For an act to constitute an offence set forth in paragraph 1, it shall not be necessary that the funds were actually used to carry out an offence referred to in paragraph 1, subparagraphs (a) or (b).
> 4. Any person also commits an offence if that person attempts to commit an offence as set forth in paragraph 1 of this article.' (parentheses added)

Article 1 paragraph 3 defines 'proceeds' as: any funds derived from or obtained, directly or indirectly, through the commission of an offence set forth in Article 2.

---

[13] Based in Vienna, this office created the UN Global Programme against Money Laundering (GPML) and the GPML Forum. See the website mentioned in footnote 14.

[14] Available on the web at <http://odccp.org/publications.html>.

[15] At pages 73 and 74

[16] Available on the web at <http://untreaty.un.org/English/Terrorism/Conv12pdf> – entry into force was 10 April 2002.

In its Article 8, the Convention refers to 'proceeds' by providing, in so far as is relevant here:

'1. Each State Party shall take appropriate measures, in accordance with its domestic legal principles, for the identification, detection and freezing or seizure of any funds used or allocated for the purpose of committing the offences set forth in article 2 *as well as the proceeds derived from such offences*, for purposes of possible forfeiture.
2. Each State Party shall take appropriate measures, in accordance with its domestic legal principles, for the forfeiture of funds used or allocated for the purpose of committing the offences set forth in article 2 *and the proceeds derived from such offences*.' (emphasis added).

The Convention does not make any explicit reference to money laundering. The closest it comes to an analogy (if it is one) is in Article 18, which provides:

'1. States parties shall co-operate by adapting their domestic legislation, including:
[...]
(b) Measures requiring financial institutions and other professions involved in financial transactions to utilize the most efficient measures available for the identification of their usual or occasional customers in whose interest accounts are opened, and to pay special attention to unusual or suspicious transactions and report transactions suspected of stemming from a criminal activity. For this purpose, States Parties shall consider:
[...]
iii) Adopting regulations imposing on financial institutions the obligation to report promptly to the competent authorities all complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or obviously lawful purpose, without fear of assuming criminal or civil liability for breach of any restriction on disclosure of information if they report their suspicions in good faith.'

Thus, for instance, proceeds arising, by whatever means, directly or indirectly, unlawfully and wilfully, from *collecting* funds with the intention that they should be used or in the knowledge that they will be used, in full or in part, to carry out a terrorist act are within the scope of the convention. It is not clear how the required element of 'unlawfulness' must be related to the collection of funds. It is clearly possible that the method used for collecting funds is not unlawful as such.

On 15 November 2000, the UN General Assembly adopted the United Nations Convention against Transnational Organized Crime.[17] This Convention is intended to close the major loopholes blocking international efforts to crack down on those engaging in illegal activities ranging from money laundering to trafficking in human beings.

---

[17] Available on the web at <http://www.odccp.org/palermo/convmain>.