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.

European Journal of Law Reform, Vol. 4, No. 2

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

local civil conflict, timber theft, or other criminal activity. Today, there is no list that evaluates whether international financial institutions have complied with basic rules of transparency or integrity. On the 'name and shame' side, there is no compilation ranking major international institutions according to their involvement in the laundering of proceeds from drug trafficking, corruption, terrorist finance, illegal logging, toxic waste, human trafficking, or corporate fraud, although such a ranking might be compiled from court documents, public investigations and press reports. Nor has there been a list involving a 'seal' or 'certificate' system by which an institution can be endorsed as having put into place a series of best practices to promote transparency.

Every year, many billions of dollars flow from international organizations and international financial institutions through the world's major international banks. These public funds are deposited and held in these private-sector institutions without considering if these institutions have put into place excellent transparency policies and procedures, or minimal ones. Indeed, such funds are deposited and held in private sector institutions that have had no due diligence or knowledge of a customer's principles, if they happen to be located in jurisdictions where such principles are either not required or are minimally enforced. The value of such deposits to the private sector financial institutions is substantial, generating not only substantial fees but the ability to engage in further lending activities of their own, due to the multiplier effect of bank deposits. To date, the only limitations placed on those holding or benefiting from such international funds has been the obligation of the institutions to account for the uses of those funds adequately. Broader obligations, such as a requirement that a particular bank implement strong guarantees of financial transparency or protective measures against money laundering, have not been demanded of private sector banks by the international organizations and international financial institutions that deposit their funds in such institutions. Rewarding private sector institutions who agree to meet high standards of transparency for the funds they process on a global basis could create a significant incentive for banks, providing additional weight to existing national efforts.

At the same time, access to the international financial services infrastructure by regions and institutions that have no controls on placement increases the world's vulnerability to terrorism. The post–11 September co-operation of Middle Eastern and other Islamic countries in tracing the funds of particular terrorists represents an important development in responding to the threat posed by terrorism in the financial context. However, 'back-end' reconstruction of particular terrorist events after they have taken place is vastly insufficient, so long as the front-door remains wide open. Controls on placement, including rigorous 'know your customer' standards, are as essential as they are culturally unlikely in many countries.

Thus, carrots and sticks need to be developed to ensure that private sector institutions in those regions have just as many incentives as do private sector institutions in countries such as Switzerland where, despite a history of bank secrecy, the need for financial transparency is now accepted. There is an obvious opportunity in this for world policy makers. The question is whether they can accept the fact that

globalized money requires not only globalized standards, but also an agreement on globalized incentives for the private sector not merely to adopt but to enforce these standards as a means to ensure their own survival.

III. Structural Consequences of the Globalization of Money

It may be self-evident that globalization has changed many practical elements of banking and financial services. However, the political consequences of globalized financial services are often not spelled out.

Prior to Globalization

Money was local. Prior to globalization and since the days when money based on something real, like shells or gold, was replaced by state-created 'fiat money', money in circulation in most countries has generally been issued by sovereign states. Alternatively, it has been issued by private sector financial institutions regulated by the sovereign state in which the institution was based. The stored value that money represents has been a value determined locally by the people within the jurisdiction that issued the currency in relation to the value of other commodities traded in that individual economy. Money was trusted locally to the extent that others would accept it in the society. To the extent that the national currency was valued at a distance by other countries, that currency would tend to be discounted, given that its principal value for the purchase of goods and services was local.

Banks were local. Although international finance is certainly not a new phenomenon, with international lending a substantial and familiar activity by the third quarter of the 19th century, most banking prior to the era of globalization and securitization was done at a local level by local banks. These local banks were largely dependent on their local community, and vice-versa, with the respective fates of the local banks and the local communities at least moderately interdependent. To go beyond the community was potentially dangerous for a bank, because of the substantial impediments to enforcing a financial obligation at a distance.

Cross-border transactions were costly and slow. Prior to the establishment of comprehensive electronic-payment systems in the last two decades, cross-border financial transactions were largely conducted on paper that required physical transport. For most transactions, the efficiencies of conducting such transactions locally would outweigh the benefits of obtaining a broader market of buyers or sellers, depositors or borrowers beyond the particular jurisdiction. In particular, uses of the offshore sector, such as the Caribbean or the Channel Islands, were limited to very large financial institutions for tax structuring and trade finance, or alternatively to small-time operators specializing in tax and creditor avoidance schemes. Access to the offshore sector was not something available to the ordinary business or citizen.

For corrupt heads of state, money moving abroad was typically hand-carried to Switzerland.

Regulators could monitor local financial services. In an environment in which most money was generated and spent locally, and not readily substituted for by other currencies in other jurisdictions, regulators were free to develop local regulatory regimes for local purposes. Some of these regimes were minimalist, others were comprehensive, and few would have met what, today, constitute the basic standards for safety and soundness. However, subject to local politics and the corruption factor, the regulatory regimes were inherently enforceable as an expression of national sovereignty. A financial institution definitively found to have engaged in unacceptable misbehaviour could be fined, lose its license, and be closed. While bank runs, bank frauds, and bank collapses remained an enduring part of the economic life of any free-market jurisdiction, enforcement at a local level was possible, and a recognized fact likely to have a substantial impact on market behaviour within the regulated institutions.

Taxes were collected at borders. Prior to globalization, the preponderant mechanism for governments to collect revenues was not by taxing income, but by tariffs, levied on goods at point of sale and, especially, when crossing borders. In such a tax regime, strong controls at the borders, including currency controls, were vital to the survival of the state, as revenue collection required the border to be a barrier before it could be a crossing. In this environment, barriers at the border, including barriers to unregulated cross-border finance, were an essential element of preserving and protecting national sovereignty.

After Globalization

Money is a global commodity. Although a government can give its currency a name and a putative value, the actual value of a currency in a globalized world is determined by global markets, private sector assessments of its value in comparison with other forms of stored value. Similar valuation is given to any particular currency the world over, regardless of location, making money a commodity whose value can be affected by the actions of the government that issued it, but not controlled by it. The loss of local control over money has meant that the valuations given to it locally may be less relevant to its strength as a durable commodity – an object that stores value – than the valuations given to it by those who have no particular stake in that currency. Being a global commodity, money may also be less susceptible to local control and regulation. As Alan Greenspan, chairman of the United States' Central Bank, the Federal Reserve, has observed: 'In the international arena [...] no overarching sovereign exists to decree what is money. Instead, a myriad of private agents must somehow reach agreement.'[2]

---

[2] 'The euro as an international currency', speech given by Alan Greenspan before the Euro 50 Group Roundtable, Washington, DC, 30 November 2001.

Banks are international. Where local banks were once dependent on local economies, international banks invest their capital wherever opportunities may present themselves, whether they are in New York, Jakarta, or Moscow. Home regulators cannot confine them, and indeed, neither can home regulation. If a local regulation appears inconvenient, it can be avoided by structuring some of the elements of the financial activity offshore. In many instances, transacting financial services offshore is more efficient and less expensive than conducting similar services on-shore. The offshore sector's minimal regulation reduces transaction costs.[3]

Regulators cannot monitor international financial institutions. The principle of home-country consolidated supervision notwithstanding, home-country regulators do not in practice audit international financial institutions internationally. They more largely rely on self-regulation and reporting by the institutions they regulate. A financial institution that does not tell the truth to its regulator about its offshore activities runs the risk of eventual exposure and punishment. In the meantime, however, there is little effective supervision. As a consequence, there has been the opportunity (and perhaps the market imperative) for financial institutions with cross-border operations to behave with relative impunity, especially in the operations they carry out in smaller, less fully regulated jurisdictions.

Borders do not block transactions. With tariffs largely gone and electronic money able to move across the planet at the speed of light, control of money at the border is largely anachronistic. Electronic currency is essentially incapable of cross-border monitoring. Cross-border movements of currency can be monitored, and countries can impose cross-border currency declaration requirements, but these requirements can be readily circumvented through alternative remittance systems that substitute netting for cross-border currency movements. To the extent that domestic regulations impose burdens involving obligations to maintain certain levels of liquidity, transparency, or payment of taxes, those with money may circumvent domestic regulations entirely through capital flight. The ineffectiveness of borders means flight capital need not truly flee. Russian oligarchs have vividly demonstrated that after illicit proceeds have been laundered elsewhere, they can be readily brought back into the home jurisdiction for reinvestment with no practical impediments to its integration into the formal financial system.

---

[3] For a detailed treatment of the development of globalized finance through the 20th century, *see* Michael D. Bordo, Barry Eichengreen, and Doulas A. Irwin, 'Is Globalization Today Really Different Than Globalization a Hundred Years Ago?' in *Brookings Trade Forum*, vol. 2 (Susan M. Collins and Robert Z. Lawrence, eds.) (Washington, DC, Brookings Institution Press, 1999), pp. 1–50; the short answer to the question in the study's title is 'yes'.

IV. Practical Impact of Globalized Illicit Finance on Political Stability and on Areas of Conflict

The integration of electronic financial payments systems into a globally ubiquitous network is of remarkably recent vintage, gathering speed in the 1980s and only reaching widespread coverage at the consumer level with the rapid proliferation of internationally linked automatic teller machines in the mid-1990s. The benefits of this integrated payments system for international businesses and travellers have been immeasurable. However, these same benefits have simultaneously worked to the advantage of those exploiting the dark side of globalization.

The Money Launderer's Common Financial Infrastructure. Global banking has provided continuing technical services to a wide range of practical destabilizers. Periodic eruptions of scandal have shown that drug and arms money launderers, diamond and timber smugglers, traffickers in people, terrorists, and corrupt officials chose a similar range of institutions to move and maintain their funds. These institutions typically include (a) small international business companies or trusts, established in jurisdictions of convenience, which establish (b) bank accounts at local financial institutions, which have correspondent banking relationships with (c) major international financial institutions, which (d) move funds willy-nilly throughout the world without regard to the provenance of the funds. Thus, over time, a taxonomy of scandals shows money laundering activity to have been facilitated, at one time or another, by Bank of America,[4] the Bank of New York,[5] Barclay's Bank,[6] Chase Manhattan (now J.P.Morgan-Chase),[7] Citibank,[8] Crédit Lyonnais,[9] Crédit Suisse, (now CSFB)[10] Daiwa,[11] Deutschebank,[12] Swiss Bank Corporation[13] (now part of UBS-AG), and Union Bank of Switzerland (now UBS-AG).[14] In some of these cases, the financial institutions may have been acting knowingly or negligently. In other cases, the institutions themselves did nothing wrong under existing laws and

---

[4] Handled proceeds of money laundering for a suspect Antiguan financial institution.
[5] Handled funds of Benex, which laundered billions of dollars from Russia, including some for Russian organized crime.
[6] Handled terrorist funds for Al-Qaeda.
[7] Handled proceeds of Colombian cocaine trafficking.
[8] Handled proceeds of Colombian cocaine trafficking, and drug-related funds from Mexico's Raul Salinas.
[9] Involved in massive financial frauds in connection with French political scandal.
[10] Involved in handling stolen funds from Philippines of Ferdinand Marcos; reportedly indicted by the Swiss government in connection with its handling of the funds of Sani Abacha of Nigeria 6 December 2000. *See* 'CS to be indicted in Abacha inquiry', *Financial Times*, 7 December 2000.
[11] Laundered funds in the Caribbean to cover trading losses.
[12] Handling terrorist funds for Al-Qaeda.
[13] Handling stolen funds from Philippines of Ferdinand Marcos.
[14] Involved in handling stolen funds from Philippines of Ferdinand Marcos.

frameworks. The fault lay not in the institutions, but rather in a system of international regulation that created neither legal norms nor regulatory mechanisms to prevent abuse.

The infrastructure for non-transparent international finance has nodes that have specialized in particular kinds of services. For example, until recently, the Bahamas and the Virgin Islands have been among the world's principal creators of anonymous international business companies (IBCs). The Channel Islands, Gibraltar, and the Dutch Antilles have been world-class centres for the establishment of trusts to hide the true ownership of funds. A single firm in Liechtenstein laundered political slush funds for ruling political parties in France and Germany; arms purchases for civil wars in Liberia and Sierra Leone; drug money for Ecuadorian cocaine trafficker Jose Reyes-Torres, and stolen funds for various West African dictators.[15] The Liechtenstein example is not unique. Financial nodes that initially provide services for one purpose, such as tax evasion, over time attract more sinister illicit purposes.

Case Study: Cyprus. Since World War II, Cyprus has provided trade finance and related services for a variety of cross-border trade and commercial activities throughout the Middle East and the Mediterranean. Many operating in this region have had practical reasons to avoid regulations in their home jurisdictions, as well as high taxes, bribes, the risk of nationalization, and political instability. Accordingly, Cyprus developed a strong financial secrecy regime, available through banking services, company formation, trusts, and related mechanisms. By the 1970s, this system had come to be used by terrorist organizations, arms dealers, Middle Eastern drug traffickers, Italian mafias, the Communist Party of the Soviet Union, and Israeli criminals, among many others. By the mid–1990s, as Cyprus sought to put into place a more transparent financial regime to prepare for entry into the European Union, many of the traditional illicit interests left the jurisdiction. Even then, elements of Al-Qaeda and much of the illicit finance that sustained Slobodan Milosevic's control of Yugoslavia and his sustained war in Bosnia and Kosovo remained embedded in Cyprus' financial institutions. Systems for transporting illicit funds, once established, become difficult to close even for a jurisdiction with strong incentives to do so.

Import and Export Fraud: Key Elements of the Financing of Illicit Timber and Conflict Diamonds. Illicit exploitation of a country's natural resources is a common feature of jurisdictions experiencing serious failures of governance. Such cases typically involve both failures of legitimacy and of capacity. The complex political question of who has the right to control a country's natural resources devolves into the simpler question of who has the capacity to exercise such control in practice. The power to gain access to natural resources, to strip them, to transport them out of the country, and to reap the financial benefits becomes the major practical requirements

---

[15] *See*, e.g., extensive material on money laundering allegations involving Liechtenstein, including excerpts from a German government report, on website: < http://www.marcos-billions.com > .

for those seeking to exploit them. The financial benefits are the major point of the asset stripping. Given the weakness of national currencies in such jurisdictions, obtaining money from beyond the jurisdiction, is the *sine qua non* of the entire enterprise. Much of the money may, in turn, remain outside the jurisdiction, functioning as a political slush or retirement fund, or returned to the jurisdiction to pay for weapons, bribes, or luxury cars.

One of the most widespread mechanisms for laundering money is the use of false import and export documentation. Through the technique of under-invoicing, corrupt exporters declare a smaller quantity of the exported good, and then typically share the proceeds of the additional 'invisible' export with their partner, usually either the importer or the shipper. Through over-invoicing, a corrupt exporter can pretend to ship goods that do not exist, as a cover for reimporting and legitimizing previously earned profits from other illicit activities. Both techniques provide effective mechanisms for facilitating trafficking in illicit commodities, such as conflict or stolen diamonds and timber. The corrupt payments, false documentation, theft of resources and evasion of controls, domestic and international, are an integrated set of criminal activities. For example, in the logging of Burma's frontier forests, the chainsaws and woodsmen would have no business without the simultaneous participation in the trade of corrupt officials and transnational logging companies, who make substantial payments through financial institutions to pay for the illicit timber.[16] Similarly, money laundering is an integrated component of all other major cross-border environmental crimes, such as CFC smuggling and toxic waste dumping.[17] Each component of the activities is essential to the success and continuation of the overall enterprise. Thus, disruption of any element of the total activity, including the ability to move funds in and out of the jurisdictions involved, becomes a substantial impediment to its viability.

Case Study: Sierra Leone. It has been said that the point of civil conflict in African countries such as Sierra Leone is not to win the war, but to 'engage in profitable crime under cover of warfare', with the major opportunities involving

---

[16] *See*, e.g., *Bangkok Post*, 26 March 1999, 'Massive Kickbacks Alleged;' 'Business Indonesia', 'Two Sawmills owned by General Assembly Member buys Illegal Logs', 2 February 2000.

[17] Within the US for example, smuggling of CFCs from outside the US into the US was estimated by a US government study to amount to 60 million pounds of CFCs between 1994 and 1997 from such countries as Mexico, Russia and Venezuela. In a series of cases, the US indicted the smugglers for money laundering violations, as well as environmental crimes. *See* EPA Enforcement Actions Under Title VI of the Clean Air Act, 'Texas Man Arrested For Smuggling Freon Into US – Arrest Underscores Federal Crackdown on Black Market in Ozone-Depleting Chemicals', 24 June 1999. Currently, China and India, both countries with essentially no money laundering laws, are the world's major source of illicit CFCs, especially to countries in the European Union, in violation of the Montreal Protocol. Detailed information on the illicit CFC trade has been brought together by the London-based NGO, the Environmental Investigation Agency.

diamonds, illicit timber, narcotics, and weapons smuggling.[18] As a consequence of the work of the British non-governmental organization Global Witness and other groups since December 1998, there has been widespread recognition that 'conflict diamonds' were fuelling civil wars in Sierra Leone and Angola. When international sanctions were put into place, the normal revenues from international trade for the participants in each country's civil wars were eliminated. Diamonds became the key currency for the criminals. The value of the diamonds increased exponentially once they were smuggled out of the region and into Western Europe for processing. Thus, the laundering of the proceeds of the diamonds was an essential component in sustaining the conflicts.

In response, a system has been established that requires a series of certificates to follow diamonds as they are transported, in an effort to establish a chain-of-custody that documents the legitimacy of such diamonds and thereby makes it more difficult for diamond sales to support civil war and vice-versa. Yet, while it has been recognized that the conflict diamonds have been largely purchased and processed in Antwerp, Belgium, home to numerous international banks, there is literally no public documentation on the nature of the money laundering involved in the conflict diamond trade. What is evident, even in the absence of data, is that banks in Belgium – not just banks in Western Africa – handled the proceeds of conflict diamonds without impediment, thereby making the business viable. Were financial institutions operating in Belgium effectively prohibited from laundering the proceeds of illicit diamonds, the value of such diamonds in Antwerp would be necessarily reduced, given the heightened risk to any financial institution processing the proceeds. The money flows continued unimpeded until DeBeers, the largest buyer of the conflict diamonds, determined that the risk to its reputation substantially exceeded any profits from transactions, and moved to create impediments to the illicit business. Money laundering regulation in Sierra Leone and Belgium, among other countries, was so weak that it never became a factor in the suppression of the business.

Case Study: Liberia. The Liberia of Charles Taylor has sometimes been termed 'a criminal state', in which the president, an escapee from an American prison, presides over a series of criminal businesses that include indiscriminate logging, looting of diamond mines, systematic theft of public funds, drug trafficking, and extortion.[19] Few substantial sources of revenue in the country have remained outside the control of Taylor and his corrupt associates. Throughout Liberia's civil war, Liberia has also remained a tax haven, offering 'flag of convenience' services in a variety of sectors,

---

[18] Ian Smillie, Lansana Gberie and Ralph Hazelton, 'The Heart of the Matter: Sierra Leone, Diamonds and Human Security', Partnership Africa Canada, January 2000.

[19] There is no authoritative estimate of Taylor's illicit wealth, although it is widely understood to come from the sale of iron ore and timber within Liberia, and diamonds obtained from Sierra Leone. *See*, e.g., 'Liberia stokes African gem war', *Financial Times*, 10 July 2000. The Sierrra Leone UN Expert Panel Report of 2000 describes Taylor's use of diamonds from Liberia as a source of personal revenue.

with the revenues being used to sustain control of the country by former dictator Samuel Doe, and currently, by Taylor. Liberia's commercial laws allow businesses from anywhere in the world to register in Liberia, with no requirement they have any physical presence in the country. Liberia's financial regime included corporations with no capital requirement, issuance of shares that need not be reported or recorded in Liberia, companies with no obligation to file annual reports, tax forms, or audit statements, bearer shares, and similar freedoms that in effect make the creation of an entity in Liberia a guarantee of worldwide anonymity and non-accountability. The US dollar is legal currency in Liberia. For years, Liberian diplomatic passports have been advertised (and actually made available) on the Internet, reflecting a regime that protects criminals outside of Liberia as well as within the jurisdiction.[20] Liberia's connections with the international payments system broke down during its civil war from 1991 through 1997. The most prominent non-Liberian financial institution, Citibank, left the country. Settlements among Liberian banks, and movements of funds from Liberia to other countries, were handled on an *ad hoc* basis. Yet throughout this period, Liberia's armies have been able to generate and use funds from beyond the country, with President Charles Taylor accumulating substantial personal wealth in the process. This phenomenon has continued to the present. For example, in November 2001, the government of Singapore sought information from the UN regarding financial and weapons transactions involving payments for weapons deliveries that used the Chase Manhattan Bank in New York to transfer some 500,000 USD to a Singapore arms trafficking company. Significantly, the firms involved in the arms transfer have also been alleged to be involved in illegal timbering in Liberia and Malaysia.[21] Separately, in looking at the impact of Taylor's involvement in prolonging Sierra Leone's civil war, the UN Panel of Experts discovered that Liberia secured weapons and made payments for weapons destined for Sierra Leone through accounts at the Standard Chartered Bank in Sharjah in the United Arab Emirates.[22]

Case Study: Cambodia. Corruption in Cambodia is pervasive and systemic, extending from low-level policemen to the top of the government. Important criminals have close links to Cambodia's government. For example, Theng Bun Ma, Chairman of the Phnom Penh Chamber of Commerce and a major financial supporter of Prime Minister Hun Sen, has been identified by the US as a major drug trafficker. A second important criminal figure associated with the Prime Minister, Yeay Phu, is chairperson of the Phea Pimech Company, Cambodia's biggest salt producer and most destructive logger.[23] Cambodia's own financial services sector is

---

[20] Personal inquiry by the author in 1997, during his service in the US Department of State.
[21] 'Singapore to probe alleged involvement of company in arms smuggling in Liberia', *Singapore Business Times*, 6 November 2001.
[22] Sierra Leone UN Export Report, December 2000.
[23] 'Cambodia's Hun Sen embracing new tycoons', *Phnom Penh Moneakseka Khmer*, 21 September 2001, pp. 1, 2 (Report by Chan Chamnan).

extraordinarily weak. Some money laundering in Cambodia nevertheless goes through its rather specialized banking system: most of Cambodia's banks are private institutions, not open to the public, existing mostly to move and launder money.[24] Other funds from illegal logging (as well as other criminal activities) are laundered in Cambodia's neighbours, particularly Thailand. Notably, Cambodian financial institutions have correspondent banking relationships with major financial institutions all over the world, including some based in Canada, France, and the United States, as well as in Korea and Thailand.[25]

Case Study: Thailand. The impact on the larger society of illicit finance can become broader than the illicit activity initially involved. In Thailand, illegal timber sales have for many years been a substantial source of funds for both politicians and corrupt law enforcement officials. Indeed, scandals involving such sales are frequently reported in the Thai press, and are elements in Thai political jockeying. In 1996, the government of Thailand began to recognize that non-drug money laundering was creating problems, and the government introduced comprehensive anti-money laundering legislation. For the following three years, the legislation stalled over a single issue: the inclusion of illicit timbering as a predicate offence for the prosecution of money laundering crimes. Finally, in 1999, Thailand's government reached a compromise and passed comprehensive money laundering legislation. The price of compromise was the elimination of illegal timbering as a money laundering crime, permitting corruption involving that activity to continue without restriction.

Drug Money and Civil Conflict. Areas where opium and coca are grown include regions where many of the world's longest-enduring civil wars and internal conflicts are taking place. Opium production has fuelled destabilizing guerrilla and paramilitary movements in Afghanistan, Burma, Lebanon, Pakistan, and Turkey. Coca has done the same in Bolivia, Colombia, and Peru. In each case, proceeds from narcotics production and trafficking became a mechanism for relatively unpopular governments, militia, or rebels to control the territory where the narcotics were produced, thereby sustaining themselves and perpetuating conflict with other forces in the jurisdiction. In each of these countries, the political and military forces have systematically taken 'tithes' or regular payments as protection money for the illicit crops, thereby gaining a resource advantage over any force that has not similarly accepted drug protection money.

---

[24] 'Paper: Banks in Cambodia involved in money laundering', *Phnom Penh Samleng Yuveakchon Khmer*, 30 March 2000, pp. 1, 3 (Report by Sophal).

[25] For example, the Cambodia bank Canadia, Ltd., has correspondent banking relationships with the Bank of America, Republic National Bank, Standard Chartered Bank, and Banque Nationale de Paris; the First Overseas Bank of Cambodia has correspondent banking relationships with HSBC, which in turn has branches and subsidiaries around the world. Given the absence of any controls on money laundering in Cambodia, it would be difficult to imagine how such correspondent banking accounts could be protected against laundering the proceeds of narcotics, illegal logging, and other criminal activities.

Case Study: Burma. In Burma, opium has perpetuated the rule of an entirely non-democratic junta, while providing the means for ethnic warlords to arm their local soldiers. At the same time, Burmese officials have used opium profits to invest in partnerships in legitimate businesses in neighbouring countries, such as Burma, Malaysia, Singapore and Thailand, reducing regional pressure for more democratic governance. Burma's repressive government has continued to generate international sanctions and impede foreign investment. Yet Burmese banks are thriving and experiencing rapid growth, fuelled primarily by funds generated from the opium trade. Prominent among Burma's 21 domestic banks are the Asia Wealth Bank, whose chairman and vice chairman are alleged to be former drug lords; the Mayflower Bank, established by Kyaw Win, a partner of the drug warlord Khun Sa; and the Kanbawza Bank, closely tied to the ruling junta and alleged to launder the proceeds of ruling party corruption.[26] Thus, the drug economy and the political control exercised by Burma's unelected leadership have proved mutually reinforcing. In turn, this economy has been sustained by Burma's ability to readily move funds to and from the rest of the world. Despite the allegations of its ownership by drug lords and its involvement in money laundering, the Mayflower Bank apparently maintains correspondent relationships with the Marine Midland Bank and American Express Bank in New York.[27] It is difficult to imagine that any US institution is not well enough situated to assess the provenance of funds from the Mayflower Bank.[28] EU sanctions against Burma were toughened in 2000, theoretically freezing the funds belonging to members of the junta and those associated with them. However, the state-owned Myanmar Foreign Trade Bank currently reports a network of over 120 correspondent banking relationships in 58 countries, so that 'banking transactions can be made with almost any country in the world'.[29] Burma's repressive government retains access to international financial institutions, irrespective of the sources of Burmese assets or international sanctions.

Case Study: Afghanistan. In Afghanistan, decades of tribal conflict have been fuelled by opium funds, with each of the major forces, including the Northern Alliance and the Taliban, taking drug money to finance their military campaigns. Opium's impact in acting as a regional destabilizer extends beyond Afghanistan. Drug-related corruption has been an ongoing problem within the Pakistan military. According to a recent French analysis, from approximately 1983 through 1998, Pakistan's military intelligence agency used heroin trafficking from Afghanistan to

---

[26] 'Above it all, Burmese banks are thriving even as the country's economy suffers its worst slump in years', Maung Maung Oo, the *Irrawaddy*, 2 February 2001.

[27] For example, Hamsa Travels and Tours of Yanon, Myanmar, which offers tourist services for Burma, currently specifies on its web-pages the use of these institutions to make payment to its account at the Mayflower Bank from the US.

[28] Existing US sanctions against Burma prohibit new investment but do not prevent financial transactions for such purposes as tourism.

[29] Myanmar Financial Structure and Exchange Arrangements, published by the Government of Myanmar, < http:/www.myanmar.com/gov/trade/fin.html > .

fund secret operations aimed at destablizing India through Muslim rebellion in Kashmir.[30] While much of the opium trade at the local level is cash-based, opium money arriving to Gulf State financial institutions from Pakistan is then transformed into electronic funds, which can be used not only to pay bribes further afield but to support terrorist activity around the world.

Case Study: Colombia. For many years, the Colombian terrorist guerrilla group, the Revolutionary Armed Forces of Colombia (FARC), has funded its military attack on the Colombian government by taking protection money in coca-growing areas. A map of regions controlled by FARC shows that they constitute rings just outside and around each of the major coca-growing regions, thereby placing the group in a position to exact a toll for the transit of the drugs by any route. The FARC has used the drug money for arms purchases, as have the major Colombian smuggling organizations. In turn, both the Colombian traffickers and the FARC use the weapons funded by the drug trade to protect themselves in their respective struggles against Colombia's elected government, perpetuating the civil war in that country. The traffickers have heavily penetrated Colombia's financial institutions and purchased a substantial number of legitimate businesses, facilitating their ability to corrupt elements of the Colombian government and reducing the efficacy of the government's efforts to enforce Colombia's laws. As drug influence increases and government capacity is weakened, the legitimacy of the Colombian government is further eroded, in turn providing a greater base for political support by disaffected Colombians for the guerrillas and the civil war. Again, as with drug money from Afghanistan and Burma, Colombian drug money exercises a negative political impact well beyond Colombia itself. For example, both Manuel Noriega of Panama and the military junta that ruled Haiti in the mid–1990s sustained control of their respective governments through drug-related corruption.

International Money Laundering and Grand Corruption. The world's kleptocrats, whether Marcos, Mubuto, Abacha, or Sukarto, have used a common financial services infrastructure to steal national wealth.[31] Grand corruption has been a prominent feature of political and social conflict or civic breakdown in Albania, Argentina, Burma, Cambodia, Congo (Zaire), Colombia, Haiti, Indonesia, Iran, Liberia, Nigeria, Panama, Pakistan, Peru, the Philippines, Romania, Sierra Leone, Yugoslavia, and Zimbabwe, among other jurisdictions. In each case, the looting of

---

[30] 1998–1999 Report on Drug Trafficking in Asia published by the Observatoire Geopolitique de Drogues or OGD, a French academic institute. Separately, former Pakistani Prime Minister Nawaz Sharif told the Washington Post in 1994 that Pakistan's army chief and the head of its intelligence agency had proposed a detailed blue-print for selling heroin to pay for the country's covert military operations in early 1991. *See* 'Heroin Plan by Top Pakistanis Alleged', *Washington Post*, 12 September 1994.

[31] This phenomenon has been labelled 'indigenous spoilation' by N. Kofele-Kale, who defines this act as an 'illegal act of depredation which is committed for private ends by constitutionally responsible rulers, public officials or private individuals', in the *International Law of Responsibility for Economic Crimes* (Kluwer Law International 1995) at p. 10.

government treasuries has involved funds or resources residing within these countries being moved from the countries to other jurisdictions through the world's major international banks. In some cases, the theft of national treasuries has been accompanied by other harmful activities, whose proceeds have been laundered by the same mechanisms. These include costly or illegal arms deals (Angola, Colombia, Liberia, Sierra Leone, Somalia, Sudan), the smuggling of diamonds used to purchase arms deals in civil wars (Angola, Liberia, and Sierra Leone), grand-scale theft of oil and timber (Burma, Cambodia, Nigeria, Russia, Thailand), illegal dumping of environmental toxics (Guyana, Suriname), and embezzlement or other abuses of funds lent by international financial institutions such as the World Bank (endemic).

Countries that during the 1990s saw their national wealth disappear to other jurisdictions at the direction of ruling kleptocrats include (from A to Z):

- Albania, decapitalized by a pyramid scheme that moved its funds to Italy and Western Europe;
- Angola, whose immense national resources vanished amid the ongoing civil war between President Dos Santos and Jonas Savimbi;
- Burma, where funds generated by narcotics, jewels, and illicit timber were exported for covert reinvestment in more business friendly environments, such as Singapore and Hong Kong, by people working with the junta;
- Cambodia, which featured similar characteristics of first generating illicit funds and then having them become flight capital under Hung Sen;
- Estonia, which found substantial amounts of its national wealth apparently transferred to Russia in the mid-1990s in a pyramid scheme arranged by a prominent banker with close ties to Latvia's then government;
- Gabon, whose oil revenues were sent offshore and handled by US financial institutions on behalf of the senior leaders who had stolen the proceeds;
- Indonesia, where billions of dollars disappeared offshore in connection with grand corruption under former dictator Suharto, with some 9 billion USD ending up in a nominee account maintained at an Austrian bank;
- Kazakhstan, where funds from oil revenues were laundered offshore for the benefit of senior leaders;
- Mexico, where the brother of president Carlos Salinas, Raul Salinas, was found to have moved hundreds of millions of dollars, representing either stolen government funds, bribes, or the proceeds of narcotics trafficking, to Switzerland;
- Nigeria, where General Sani Abacha stole billions that were then stored in major banks in Luxembourg, the U.K., Liechtenstein, Switzerland and the Channel Islands, among other locations;[32]

[32] *See*, e.g., 'Swiss banks criticised over Nigerian funds', *Associated Press*, 5 September 2000, describing findings of the Swiss Federal Banking Commission regarding the handling of some 670 million USD of funds stolen by Sani Abacha and his 'entourage' from Nigeria and held by 19 Swiss banks. According to the article, the Government of Nigeria says the total funds stolen by Abacha amounted to some 3 billion USD, some of which remained in other accounts in Belgium, Germany and France.

- Pakistan, where military rule replaced democratic civilian rule after hundreds of millions of the proceeds of corruption were found in Swiss banks, discrediting the elected Prime Minister and her family;
- Russia, whose financial system collapsed in 1999 amid massive money laundering overseas through the Caribbean, the South Pacific, New York, and London;
- Serbia, whose wealth was converted to the control of Slobodan Milosevic and his wife through such jurisdictions as Cyprus and Lebanon, while Serbia was subject to global sanctions by the United Nations;
- Ukraine, where substantial stolen assets of the state under the control of a former prime minister were found to have been laundered to the United States, after being handled by a number of Swiss banks;[33]
- Zaire (Congo), whose national wealth was exported by the late dictator Mobuto to Swiss banks.

Thus, a wide variety of serious problems of governance have been facilitated by illicit finance, which in turn leads back to the problem of the 11 September terrorist attacks, where money from apparently legitimate sources, such as wealthy Muslims in the Persian Gulf seeking to support Islamic charities, was turned to horrific ends after passing invisibly through the pipes of the world's global financial service infrastructure.

V. Terrorist Finance and Civil Conflict

International terrorism represents an obvious threat to global security, just as domestic terrorism does to many individual nations. In every case, terrorist organizations need to generate, store, and transport funds, often across borders. While not every domestic terrorist organization needs to launder money through cross-border transfers, over time, many such organizations choose to locate portions of their infrastructure at some distance away from planned terrorist activities. To do so, they establish cells to operate in jurisdictions separate from those where their political base is or where their operations will be carried out. In recent years, multinational movements of terrorist funds, involving the use of major international financial institutions, have been traced to terrorist movements based in Afghanistan, Burma, Chechnya, Colombia, Israel, the Palestinian Territory, Kosovo, Lebanon, Northern Ireland, Pakistan, Papua New Guinea, the Philippines, Somalia, Sri

---

[33] *See US* v. *Lazarenko*, Northern District of California, superceding indictment, 23 July 2001, describing Lazarenko's use of SCS Alliance, Banque Populaire Suisse, Crédit Suisse, Crédit Lyonnais (suisse), and European Federal Credit Bank in Antigua to launder 21 million USD stolen from Ukraine.

Lanka, Sudan, and Turkey. Although the terrorist organizations based in each of these countries have some level of minority popular support, their power and effectiveness have been leveraged by their ability to hide, invest, and transport their funds through the world's international financial institutions. A summary of the nations whose banks have been used to handle funds for Al-Qaeda's attacks on the US is instructive in this regard. Available public sources show Al Qaeda and related groups to have been able to move funds to institutions in the following countries: Albania, Australia, Austria, the Bahamas, Belgium, Canada, the Caymans, Cyprus, France, Germany, Greece, Hong Kong, Indonesia, Iraq, Italy, Kosovo, Kuwait, Libya, Macao, Malaysia, Malta, Mauritius, the Netherlands, Nigeria, Panama, Pakistan, the Philippines, Poland, Qatar, Saudi Arabia, the Seychelles, Singapore, Somalia, South Africa, Sudan, Switzerland, the United Arab Emirates, the United Kingdom, the United States, and Yemen. Significantly, where these jurisdictions are used by Al Qaeda, they also tend to be used by other criminals and corrupt officials, as the case of the United Arab Emirates demonstrates.

Case Study: United Arab Emirates. The UAE houses the Middle East's most sophisticated financial services sector, which is intensely competitive and lightly regulated. It is also a cash-intensive society, with Dubai constituting the regional gold centre. Cash transactions at restaurants, hotels, nightclubs, money-exchange houses, and investment firms remain common and effective mechanisms to launder money throughout the world from the UAE.[34] Trading in precious metals, especially gold, has been simultaneously implicated in tax frauds, money laundering, organized crime, and the smuggling of stolen cargo from the UAE.[35] Islamic banks, once a conservative mechanism for relative low-cost entry into the international financial system, have expanded rapidly, remaining little regulated beyond the requirements of Islamic shari'a. Alternative remittance houses, such as hawalas, have been abundant, and scarcely regulated. The results for global security were evident in the 11 September terrorist attacks. One hawala based in Somalia, Al Barakaat, with major offices in the UAE, was found to have been heavily involved in funding Al Qaeda's global operations. Another unnamed money changer was found to have transferred funds to Marwan Al-Shehhi, a UAE citizen who was the suspected pilot of United Airlines Flight 175, the second plane to hit the World Trade Center on 11 September.[36] In addition, funds were allegedly wired between three of the terrorist attackers and one of Bin Laden's financial chiefs, Shaykh Said, also known as Mustafah Muhammad Ahmed, who resided in Dubai until 11 September, according to numerous press accounts.[37] Subsequent press accounts traced the funds to the Al

---

[34] 'Dubai Police Study on Money Laundering', Khalij Times, December 10, 1999.

[35] 'Duped banks get wise to crime' Lloyd's List, January 8, 2001.

[36] 'UAE Central Bank Withdraws License of Money Changer', *Wall Street Journal*, 2 November 2001.

[37] *See*, e.g., 'In Emirates, An Effort to Examine Bank System', *New York Times*, 15 October 2001; '$100,000 trail links hijackers to Al-Qaeda, sleuths say', *Dubai Gulf News*, 12 October 2001.

Ansari Exchange branch in Abu Dhabi.[38] Another account cited an unnamed US intelligence official as stating that two of Bin Laden's sisters used the UAE as a transit point for shuttling cash to Bin Laden and his hide-out in Afghanistan.[39]

Long before the 11 September terrorist attacks, the UAE's financial system was repeatedly linked to terrorist finance. Al Qaeda also used the Dubai Islamic Bank as a mechanism to process funds used in the bombings of the US embassies in Kenya and Tanzania in 1998.[40] UAE financial institutions were central to the 11 September terrorist attacks on the US financed by Osama Bin Laden and Al-Qaeda. UAE institutions were also reportedly used by other Bin-Laden terrorist finance operations based in Malta.[41] This terrorist finance infrastructure overlaps substantially with other money laundering operations. For example, the same networks in the UAE have been used to launder drug money[42] and to handle the proceeds from Russian criminal activity, in one account, laundering some 300 million USD in Russian funds in the month of January 1999 alone.[43] The UAE has been home to the Russian arms merchant Viktor Bout, implicated in black market weapons sales to Rwanda, Sierra Leone, and Angola. False end-user certificates were delivered from the UAE to provide a veneer of legality to Bout's illicit arms sales, according to a United Nations report. Bout's illicit arms shipments were carried out from the UAE through his UAE-based air transport company, Air Cess, whose operations would clearly require financing through the UAE.[44] Even as Bout engaged in smuggling activities to these jurisdictions in conflict, UAE financial institutions handled the proceeds to finance terrorist and criminal activity. For example, Al Qaeda used diamonds purchased in Sierra Leone, the Democratic Republic of the Congo (DROC, the former Zaire) to fund its activities, in turn laundering these commodities through Dubai.[45]

Ironically, throughout this period the UAE had one of the Middle East's *best* anti-money laundering regimes, as well as a good reputation for co-operation in particular cases arising from investigations in other countries, including the US. Yet

---

[38] 'UAE Central Bank Withdraws License of Money Changer', *Wall Street Journal*, 31 October 2001.

[39] 'United Arab Emirates emerges as key link in money trail that led to attacks', *Knight Ridder Washington Bureau*, 2 October 2001.

[40] 'UAE Bank Sources Deny Knowledge of Bin-Ladin Dealings', *London Al-Sharq al-Awsat* (in Arabic), 9 July 1999, p. 5.

[41] 'Malta's Central Bank Asked to Investigate Possible Bin-Ladin Financial Assets', *London Al-Sharq Awsat*, 16 November 2000.

[42] *Financial Times*, 24 February 2001.

[43] 'Capital Flight, Money Laundering Eyed', *Moscow Noryye Izvestiya* (in Russian), 5 March 1999.

[44] 'The Great Small-Arms Bazaar', *Cox News Service*, 6 July 2001; 'UN Report: Former Russian KB Officer Arming African Rebels', *London Guardian*, 23 December 2000.

[45] 'Al Qaeda's Road Paved With Gold, Secret Shipments Traced Through a Lax System in United Arab Emirates', *Washington Post*, 17 February 2002 (Douglas Farah), citing US and European intelligence sources and investigators.

the rules had proven to be largely helpful in reconstructing money laundering or terrorist finance after a crime had taken place, rather than deterring it in the first place. Moreover, the UAE had a wide range of financial links to other jurisdictions, from Pakistan to Iran, that had essentially no anti-money laundering regimes in place, making it easy for illicit funds to be placed elsewhere before moving through the UAE and into Western Europe, North America or Asia. Further, Dubai, the most developed financial centre in the UAE, was the world's centre for trading in gold, as well as a central component of the hawala alternative remittance system. With gold trading, drug-money launderers and terrorist financiers alike could move funds through the UAE. With hawalas, the same interests could move money to wherever they needed it without the funds ever having to move across international borders.

VI. The Commingling Problem

The world's networks of non-transparent financial services not only commingle licit with illicit funds, thus rendering the illicit funds more difficult to detect, but also provide vessels for the intermingling of different forms of illicit activity, which have the common element of being both destabilizing and involving similar persons and institutions. The ubiquity of offshore havens such as the Caymans, Channel Islands and Liechtenstein for common use by drug, arms, and people traffickers as well as kleptocrats is reasonably well understood. The interconnections between Al Qaeda's terrorist finance and the illicit sale of diamonds mined by rebels in Sierra Leone is less obvious, although increasingly well-documented and tied to other terrorist finance of groups such as Hezbollah. Within the region, the diamonds are transferred to the terrorists in return for weapons or for cash. The terrorists then transport the diamonds to diamond processing centres such as Belgium, and thereby launder their funds anew for further terrorist activity.[46] Neither the diamond dealers of Antwerp nor the financial institutions that serve them currently have in place any trip-wires that would alert them to the possibility that either the diamonds, or their owners, were involved in funding destabilizing conflict in western Africa or global terrorism.

The problem is not necessarily one of witting intention on the part of the parties who populate the vast infrastructure supporting many of the world's most destabilizing illicit activities. Rather, the global money-laundering problem is a structural consequence of globalization, putting bankers, banks, and banking accounts in constant contact with people and businesses that they do not know.

---

[46] 'Al Qaeda Cash Tied to Diamond Trade', *Washington Post*, 2 November 2001 (Douglas Farah), citing US and European intelligence officials.

Instead of having relationships with people they trust, these institutions have accepted the notion that they should trust only in the money itself, with no further obligation.

Twenty years ago, the risks posed by 'no-questions asked' banking practices were not universally evident. Now the need for greater transparency, accountability, and traceability of financial transactions, regardless of their provenance, destination, or the mechanics of their movement, is widely accepted. Within the past two years many countries, in some cases threatened with possible loss of access to major financial centres, have enacted comprehensive measures to combat money laundering and to promote financial transparency. These countries have included Antigua, Austria, the Bahamas, the Channel Islands, Israel, Japan, Liechtenstein, Panama, Russia, and the United Arab Emirates. The 11 September terrorist attacks on the United States have led to a further wave of legislation and regulation. The result has been closer financial scrutiny of many Gulf States, a number of countries in Southeast Asia, and of the placement of funds in jurisdictions in the Americas and Europe. This new scrutiny has included the first comprehensive efforts to understand, register, and regulate alternative remittance systems or hawalas.

Yet, governments whose jurisdictions begin and end at their own borders may be poorly placed to exercise effective oversight of private sector financial institutions whose activities may extend through many dozens of jurisdictions. If individual nations are incapable of exercising authority over the global operations of the financial institutions they license, there is an obvious question as to who is in a position to exercise such authority. One answer – the market shall rule – is clearly incompatible with other important social, economic and political goals. A second answer, that the institutions will regulate themselves, has to date not proven very effective. Soft standards (typically guidelines), imposed by self-regulatory organizations such as the BCBS, IOSCO, and the IAIS, have given national regulators responsibility to decide on sanctioning cases of institutional misbehaviour, and this too has not proven very effective.

Each of the many exercises seeking to improve international financial regulation and to oppose illicit finance has adopted one core principle, a principle of particular import in an age of globalization. This principle, sometimes summarized as 'know your customer', suggests merely that the obligation of knowing with whom you are doing business, a matter of prudence in a local economy, becomes even more essential in a global economy. There is no disagreement on this core standard, only a clear failure to date to impose it on a universal basis. Assessing the existing and potential mechanisms for implementing this principle take up the remainder of this paper.

VII. Existing Initiatives

As Brookings Institution economist Robert Litan has recently stated, successful international efforts to regulate cross-border finance generally only emerge in response to crises.[47] The sheer scope of the existing anti-money laundering initiatives provide some evidence of the depth of the global financial transparency crisis.

The major financial services jurisdictions, including the countries of the G–8, the EU and Switzerland, have already begun to implement financial regulatory regimes based on the premise that the best possible protection against being victimized by financial crime of any kind is to know the true identity and business of any party to whom one is exposed in a transaction, from one's customer to one's correspondent bank. This principle is embedded in the work of the G–7 Financial Stability Forum, of the EU's Second Directive on Money Laundering, agreed to in October 2001, and in the USA-PATRIOT Act, enacted by the US to counter terrorism and terrorist finance in the wake of the 11 September attacks. These new legal regimes no longer treat all bank accounts as inherently equal, but require those who handle the funds of others to know who the beneficial owner of an account is, regardless of the nature of the account. In cases where an account is established through a jurisdiction that is inadequately regulated or designed to hide beneficial ownership, these regimes would shut off access entirely, as the new law in the US has required them to do since the end of 2001.

Know Your Customer. The principle of 'know your customer' is now true not only for banks but for all financial intermediaries engaged in transnational financial activity, especially that which is electronic. In the age of the Internet, no other approach is workable. If merely banks are regulated, and their non-bank competitors are not, the competitors will engage in unregulated bank-like activity. To be effective, the 'know your customer' requirements of the original Basel Committee recommendations of a decade ago are now slowly being updated and broadened to cover those who offer banking-like services. Jurisdictions that lag behind in undertaking this approach, either through self-regulation, government regulation, or a mixture of the two, are finding themselves and their financial institutions at risk of having reduced access to other jurisdictions. The result has been a jurisdictional regulatory 'race to the top', instead of a race to the bottom. Nevertheless, the emerging new international instruments, standards, and initiatives have yet to have a substantial impact in reducing global conflict.

Naming and Shaming Jurisdictions. A common feature of the major initiatives undertaken to date by governments, international organizations, and non-governmental organizations, such as Transparency International, has been a focus on reforming governments, and through the reform of the governments, enhancing regulation and oversight of the private sector. Existing international instruments to combat money laundering include the 1988 United Nations Vienna Convention

---

[47] Litan, id, p. 197.

Against Illicit and Psychotropic Drugs, the 2000 United Nations Convention Against Transnational Organized Crime, the 1998 OECD Convention Against Illicit Payments (covering bribery), and numerous instruments enacted by the Council of Europe, the Organization of American States, and other regional groupings. Over time, these international instruments have come to create a body of international standards, embedded in the increasing number of mutual assessment mechanisms. The first and most successful of these remains that undertaken by the FATF and its progeny. In recent years, failures to meet these standards have even come to have consequences, as specific jurisdictions have been named, shamed, and in effect forced to change their laws in order to avoid risks to their economies, political regimes and reputations. However, in many countries, governments simply do not control the private sector, and globalization has made cross-border control inherently impossible even for the most powerful governments. International regimes that direct governments to regulate private sector institutions that may be more sophisticated, more international, wealthier, and larger than the governments purporting to regulate them have inherent practical limits.

The nature of these limits is already visible, as the name and shame exercises have taken hold. While individual jurisdictions have been forced to change their rules, individual institutions have been able to continue to engage in regulatory arbitrage, pushing their riskiest and least attractive transactions to jurisdictions that require the least transparency. For example, during the last half of 2001, the tiny Channel Island of Jersey was found to house millions of dollars stolen from investors in the Gulf States by a Hong Kong-based investment company;[48] 200 million USD allegedly looted from Brazil in a major political scandal, deposited in a branch of Citibank;[49] and some 300 million USD in accounts belonging to the late Sani Abacha, his family and entourage. Jersey was in compliance with all of the FATF anti-money laundering criteria, and most of the obligations required by the OECD tax haven exercise. Yet the persistence of Jersey's use to conceal financial crime reflected the reality that anyone who deliberately structured their transactions across multiple jurisdictions was still able to protect their illicit activities from scrutiny for a very long time. The problem may not in fact be with Jersey's ability to enforce its anti-money laundering regime, but with the inadequacies of regulators and law enforcement agencies the world over to keep track of the transnational activities of the private sector entities that they purport to oversee.

Just as globalization has caused even the smallest, local financial jurisdiction, such as that of Jersey or Liechtenstein, to be accessible for use by any and all of the world's businesses, legitimate and illegitimate, the same phenomenon has required the extension, bit by bit, of regulation from its initial application to limited problems in limited sectors to universal problems in all sectors, as the evolution of the FATF and the OECD Harmful Tax Practices initiatives have demonstrated.

---

[48] 'UAE: Investment Firms Defraud Investors', *Dubai Khalej Times*, 21 August 2001.
[49] 'Brazil scandal hits Citibank', *The Observer*,9 September 2001.

The Financial Action Task Force. The FATF was established during the French presidency of the G-7 in 1989 in response to the G-7's recognition of the threat posed to banking and financial systems by drug money laundering. At the time, drug money laundering in the Americas emanating from Colombia were fresh in the minds of policy-makers, following the crisis between the US and Panama that ended with the removal and arrest of General Manuel Noriega. The FATF's initial mandate was to examine the methods used to launder criminal proceeds and to develop recommendations for combating them. These 40 Recommendations, developed during the FATF's first year, in turn, became the basis for what was then an innovative system for implementation. The FATF, which had a tiny secretariat and was not a chartered international organization but only a voluntary association, initiated a system for self- and mutual assessment. Under this system, each member of the FATF would first assess its own compliance with the FATF's 40 recommendations. Then, other FATF members would visit the jurisdiction, question authorities from the assessed jurisdiction, and reach their independent determination of where the jurisdiction was failing to meet the standards of the 40 recommendations. This approach had several ground-breaking aspects. First was the notion that technical experts could develop standards which over time would bind their countries in practice even in the absence of their entering into a formally binding international agreement. Second was the concept of mutual evaluation, in which a country would submit to peer review as a means of improving its domestic capabilities. Each of these developments faced potentially substantial risks. For example, the withdrawal of any FATF member from consensus on the standards could have had the impact of undermining both the legitimacy and effectiveness of the entire initiative. Similarly, the politicization of the mutual assessment process, either to exculpate unfairly or to criticize unfairly any jurisdiction, could also have fatally impaired the FATF's legitimacy. Both risks were avoided largely because of the technocratic nature of the staffing of the FATF by member governments. The FATF process was driven by technocrats from finance ministries, regulators, and law enforcement, not by foreign ministries or political figures. Its standards were neutral, and its judgments, initially confidential, were recognized to be fair. Moreover, the FATF proceeded slowly, first evaluating jurisdictions with robust regulatory and enforcement regimes, criticizing them, and only then moving to jurisdictions that diverged further from the 40 recommendations.

The FATF moved forward steadily but slowly during the 1990s, in the process taking on two major changes to its original mandate. In 1996, under the US Presidency of the FATF, the organization expanded its mission beyond reviewing capacities against narcotics money laundering to cover all money laundering involving all serious crimes. It also agreed to take on new developments in money laundering trends, especially those involved with electronic fund transfers. Secondly, the FATF decided that the ability of its member jurisdictions to protect themselves against money laundering would be undermined if non-member jurisdictions did not adopt and implement its 40 recommendations as well. Accordingly, it chose to move beyond its initial mandate to assess its own members to develop a 'black list' of other

countries whose practices were deemed to facilitate money laundering and therefore be 'non-cooperative' with the objectives of the FATF. The development of a black list reflected a dramatic change in approach by the FATF, necessitated by the growing recognition of the interdependence of the global financial infrastructure, and the inability of any jurisdiction to protect itself in the face of bad practices in other jurisdictions.

Both the FATF's standards and its selection of non-cooperative jurisdictions illustrate the nature of transnational money laundering and the practices most likely to facilitate it. Core FATF standards include:

1. Criminalizing the laundering of the proceeds of serious crimes and enacting laws to seize and confiscate them.
2. Obliging financial institutions to identify all clients, including all beneficial owners of financial property, and to keep appropriate records.
3. Requiring financial institutions to report suspicious transactions to competent national authorities and to implement a comprehensive range of internal control measures.
4. Putting into place adequate systems for the control and supervision of financial institutions.
5. Entering into agreements to permit each jurisdiction to provide prompt and effective international co-operation at all levels, especially with regard to exchanging financial information and other evidence in cases involving financial crime.[50]

In general, these standards have been little changed since their development in 1990. Nevertheless, they remain incompletely implemented internationally, prompting the FATF to develop in 2000 its list of 'Non-Cooperative Countries and Territories'. Four of the countries on the original list, Bahamas, Cayman Islands, Liechtenstein, and Panama, enacted comprehensive money laundering regimes rather than face the risk of possible loss of market access to FATF Member States if they failed to take action. Others, such as Israel and Russia, enacted legislation, but failed to put in place an anti-money laundering system sufficient to meet FATF standards. To date, the FATF has threatened a number of jurisdictions with the sanctions of facing enhanced scrutiny or greater regulatory barriers, but has imposed them on none. The simple threat has been enough to cause any country targeted with immediate action to change its laws, as Austria, the Seychelles, and Turkey demonstrated even prior to the Non-Cooperative Countries and Territories initiative.

Currently, 19 countries and territories are on the FATF black list, facing the risk of potential sanctions, termed 'countermeasures' by the FATF in the near future. The list of these jurisdictions, with annotations by the author about the type of money laundering involved, is as follows:

---

[50] The full text of the FATF's 40 Recommendations is available at the FATF's website online at <http:/www.oecd.org/fatf>.

1. Cook Islands, used by Russian criminals to loot Russia.
2. Dominica, providing false identities, passports, and banking services to Russian criminals and drug traffickers.
3. Egypt, a centre for financial fraud and possibly terrorist financing; has had no transparency or anti-money laundering laws, so data is extremely limited.
4. Grenada, false identities and banking services to financial criminals and drug traffickers.
5. Guatemala, exploitation by drug money launderers.
6. Hungary, comprehensive banking secrecy exploited by Russian organized crime involved in trafficking of women, alien smuggling, and contraband smuggling.
7. Indonesia, money laundering for illicit timber, massive corruption and fraud.
8. Israel, money laundering for Russian organized crime, including trafficking in women.
9. Lebanon, laundered funds for sanctioned regimes including Libya and Serbia, as well as for various terrorist organizations; handles proceeds of drug trafficking from Middle East.
10. Marshall Islands, used by Russian criminals.
11. Myanmar (Burma), wide open to narcotics money laundering, arms trafficking, illicit timbering, precious gems smuggling, and the funding of private armies.
12. Nauru, principle launderer for theft of Russian national resources.
13. Nigeria, drug money laundering, major financial crime, terrorist finance.
14. Niue, handled Russian money laundering.
15. Philippines, laundered funds for Al Qaeda.
16. Russia, wide open to money laundering by Russian, Colombian, and Italian organized crime, including the proceeds of corruption, theft, drug trafficking, trafficking in women, people smuggling, stolen motor vehicles, intellectual property crime, extortion, and massive fraud.
17. St. Kitts and Nevis, handled drug money laundering.
18. Ukraine, laundered proceeds of corruption, trafficking in persons, theft of national resources, drugs.

Notably, none of these jurisdictions is as yet isolated from the world's major financial markets, although a few, especially those in the South Pacific, no longer have relationships with some large international financial institutions since the exposure of the Bank of New York/Benex scandal in the fall of 1999.

The OECD Harmful Tax Practices Initiative. As of the late 1990s, the growing recognition that lack of transparency was creating substantial problems even for the most affluent countries as a result of globalization began to embrace the area of taxes. Finance ministries of the OECD countries had come to conclude that they were losing exceptionally large amounts of revenue due to individuals and companies engaging in systematic tax evasion through structuring their activities cross-border and taking advantage of banking secrecy regimes. Previously, the OECD had

focused on eliminating regulations that could impede international trade or impose market distortions. Its senior officials came to see what it termed 'tax poaching' as a practice increasingly undermining the revenue base of governments throughout the world, reducing their ability to raise revenues and provide fundamental services. In short, the OECD saw that globalization led to tax evasion and, in turn, undermined fundamental governmental capacities to govern. As the OECD studied the problem, it also came to recognize that international tax evasion was linked to a host of other serious threats to the global system. In the words of OECD's Secretary General, Donald J. Johnston, 'there are strong links between international money laundering, corruption, tax evasion, and other international criminal activities. These illegal activities are widespread and involve such sizeable sums that they can pose a threat to the stability of the global system of finance and even the global trading system'.[51] Notably, the OECD was not focused on weaker jurisdictions involved in civil conflict, but on the impact of financial secrecy in the tax arena on the world's *strongest* jurisdictions.

In May 1998, the OECD governments issued a report on 'Harmful Tax Competition', which led to the creation of a 'Forum on Harmful Tax Practices', a set of 'Guidelines for Dealing with Harmful Preferential Regimes in Member Countries', and finally, a series of Recommendations For Combating Harmful Tax Practices. The initiative was built, in many ways, on the parallel work of the FATF, and, in particular, three elements of FATF's approach. First, the OECD developed a set of agreed standards to combat a set of agreed problems; secondly, the OECD put into place a system for the multilateral assessment of each jurisdiction's implementation of the agreed standards; thirdly, the OECD adopted a 'name and shame' approach, creating a black list of jurisdictions that would face loss of market access or other sanctions if they did not take action. Despite vigorous protests from smaller jurisdictions that had been engaged in 'ring-fencing', the practice of promising little or no regulation and taxation of funds from overseas, as distinct from the regulation and taxation of the funds of their own citizens, targeted jurisdictions rapidly enacted new regimes. To avoid being placed on a prospective black list, six prominent tax avoidance jurisdictions, Bermuda, Cayman Islands, Cyprus, Malta, Mauritius, and San Marino, committed themselves in June 2000, in advance of their assessments, to embrace international tax standards for transparency, exchange of information and fair tax competition prior to the end of 2005. It may be useful to list the fundamentals of the OECD standards, as each of them applies to the lack of transparency common to all money laundering, not merely those pertaining to tax crimes:

1. Ensuring that information is available on beneficial (that is, actual) ownership of companies, partnerships and other entities organized in the jurisdiction.

---

[51] 'Introductory Remarks of the Honourable Donald J. Johnston, Secretary-General of the OECD, High Level Symposium on Harmful Tax Competition', 29 June 2000.

2. Requiring that financial accounts be drawn up for companies organized in the jurisdiction in accordance with generally accepted accounting standards, and that these accounts be appropriately audited.
3. Putting into place mechanisms so that the jurisdiction is able to share information pertaining to tax offences with corresponding authorities in other jurisdictions.
4. Ensuring that its regulatory and tax authorities have access to bank information that may be relevant for the investigation or prosecution of criminal tax matters.

The OECD's insistence that such fundamental, common sense principles be adopted has produced substantial controversy in many historic tax havens, including a number of smaller jurisdictions in the Caribbean and South Pacific. The resistance to their universal adoption is itself evidence of how badly their adoption is needed, and of the degree to which basic elements of financial transparency have yet to be put into place at the international level.

The Wolfsberg Principles: A Private Sector Alternative. Abuses of private banking by corrupt officials became substantially exposed in the late 1990s, in the course of changes of government and exposures of individual kleptocrats as described above. In each of these cases, highly-placed political officials were found to have laundered inexplicably large sums of cash through major international financial institutions that had been, at the least, incurious as to whether the sources of the funds involved were legitimate. In response, twelve of the largest international banks and the anti-corruption organization Transparency International (TI) undertook an initiative in 2000 that led to their development and adoption of 'Global Anti-Money Laundering Guidelines for Private Banking'. These guidelines, endorsed by the participating global banks in October 2000,[52] were intended only to apply to private banking, that is, to the accounts of the extremely rich, those with deposits of 3 million to 5 million USD. Lacking any oversight mechanism, they were to be self-regulatory guidelines to which each subscribing institution would adhere. The lack of an oversight or assessment mechanism for the Wolfberg Principles has led to some criticism. However, the eleven Wolfberg Principles established for the private banking sector by the twelve international banks are themselves of great significance, illustrating both potential solutions and aspects of the nature of the continuing problem in discouraging the criminal and the corrupt from taking advantage of world's global financial infrastructure. They are:

1. Adopting client acceptance procedures so that the banks accept 'only those clients whose source of wealth and funds can be reasonably established to be

---

[52] The participating banks, known as the Wolfsberg Group, consist of ABN Amro N.V., Banco Santander Central Hispano, S.A., Bank of Tokyo-Mitsubishi, Ltd., Barclays Bank, Citigroup, Crédit Suisse Group, Deutsche Bank AG, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, and UBS, A.G.

legitimate'. These procedures are supposed to include: (a) taking reasonable measures to establish the identity of its clients and beneficial owners before accepting money; (b) demanding adequate identification before opening an account; (c) determining the source of wealth, the person's net worth and the source of the person's funds; and (d) requiring two persons, rather than just one, to approve the opening of an account.

2. Engaging in additional diligence or attention in cases involving the use of numbered or alternative name accounts, high-risk countries, offshore jurisdictions, high-risk activities, or public officials.
3. Updating client files when there are major changes in control or identity.
4. Identifying unusual or suspicious transactions, following them up, and then deciding whether to continue the business relationship with heightened monitoring, ending the relationship, or advising authorities.
5. Monitoring accounts through some means.
6. Developing and implementing a 'control policy' to insure compliance with bank rules.
7. Establishing a regular method of reporting on money laundering issues to management.
8. Training bank employees involved in private banking on the prevention of money laundering.
9. Requiring the retention for at least five years of bank records that might be material to anti-money laundering matters.
10. Establishing an 'exception and deviation procedure that requires risk assessment and approval by an independent unit' for exceptions to the previous nine principles.
11. Establishing an anti-money laundering unit at the financial institution.

The head of TI, Peter Eigen, introduced the principles at the time of their adoption in terms that highlighted the historic problem of bankers being willing to handle the proceeds of corruption, describing the creation of the Wolfsberg Group as a 'unique event' because 'few would expect the leading anti-corruption organization and the leading banks to be standing on the same platform'. Dr. Eigen further stated that the Wolfsberg Principles 'state unequivocally that banks agree they should not be used by corrupt crooks and that it is fully incumbent on individual banks to put into place fully effective systems to ensure that their institutions are not money laundering vehicles. The language is blunt. The burden for monitoring the implementation and day-to-day operations of the guidelines rests squarely on the banks. Their reputations are at stake'.[53] In short, the Wolfsberg Principles would have an impact because an institution that had subscribed to it would have its reputation hurt if it failed to then meet its public commitments.

---

[53] Opening Statement, Dr. Peter Eigen, Chairman, Transparency International, 30 October 2000, available at <http://www.transparency.org>.

The universal adoption of each of the above principles, with the exception of number 10, would contribute to making it harder for corrupt officials or drug traffickers to establish accounts with funds of unknown provenance. Yet in specifying their agreement to adopt these principles, the signatory international banks are necessarily implying that, previously, such principles may not have been adopted by them on a universal basis, although each has already been either expressly or implicitly required by the 40 recommendations of the FATF.

Notably, the banks subscribing to the Wolfsberg Principles did not commit to applying them to all of their accounts, but only to their private banking departments. Moreover, principle number 10, exceptions and deviations, contemplates the possibility that such principles as knowing the customer, reporting suspicious transactions, or maintaining records might not be followed if the bank decided there was an appropriate reason for ignoring the rule. Left outside the parameters of the Wolfsberg Principles entirely are such other areas as correspondent banking involving high-risk jurisdictions. Also left outside the parameters of the Wolfsberg Principles are the hundreds of large international banks that have yet to endorse them, as well as the thousands of mid-sized financial institutions with multi-jurisdictional operations. Important components of the world's financial services sector are also missing from the members of Wolfsberg Group, which does not include a single institution based in China, Russia, Latin America, Africa or the Middle East. The absence of outside assessment or oversight for the Wolfsberg Principles and its members, illustrates the limits of this initiative, and the distance yet to be traveled before there is general acceptance of universal anti-money laundering standards among the world's interlinked financial institutions.[54]

Nevertheless, the Wolfsberg Principles remain an important development: lacking the mutual assessment mechanism and the comprehensiveness of the FATF mechanism. They demonstrate that, in the absence of globally-applicable agreements by private sector institutions, even widely accepted principles such as those of the FATF may remain incompletely adopted. So long as regulatory arbitrage remains available on an international basis, general agreement among most countries to adopt standards does not prevent private institutions from adhering to the standards

---

[54] *See*, e.g., editorial of the Financial Times, 30 October 2000, 'Banks Clean Up', stating that 'it may be surprising that 11 of the world's biggest banks should find it necessary to declare that they are opposed to the use of their networks for criminal purposes. Yet a series of scandals has shown how corrupt politicians and other criminals have found it easy to launder their loot through the international banking system[...]The bad publicity stemming from such disclosures has persuaded the 11 signatories that the damage to their reputations of becoming involved, however inadvertently, in money-laundering is greater than any financial benefit[...]but ending the flows needs the involvement of the whole financial services industry including the host of other institutions whose transactions can help hide criminal plunder. The next step is for the financial regulators to adopt the Wolfsberg principles for the organizations they supervise and closely monitor their enforcement'.

only in those jurisdictions that require them. Broader, global adoption of the standards requires commitments from the private sector institutions that these standards apply everywhere, not merely where there is a good local regulator.

A set of mandatory rather than optional principles, adopted by the world's major financial institutions on a global basis, would have the potential of transcending the limits of individual national regulators, especially were it to become applicable to all financial service sector operations, rather than only to private banking, and to become subject to assessment and oversight mechanisms by outsiders on a global basis. Indeed, the UN already relies on the principal of private sector implementation and co-operation in its handling of sanctions.[55]

VIII. Global Standards for the Private Sector: Adopting A White List Regime

The largest financial institutions of the world operate in dozens of jurisdictions. Even smaller financial institutions are networked in practically all jurisdictions. This networking appears to be largely viable, even when countries face international sanctions, as either sympathetic jurisdictions or financial institutions provide ongoing financial services to those theoretically sanctioned and off-limits.

The largest international financial institutions remain the most important nodes in the world's financial service infrastructure. Yet to date these institutions and those competing with them have continued to take advantage of the substantial regulatory and enforcement arbitrage afforded by the differences in government laws and capacities to launder the illicit proceeds of the world, and thereby to facilitate the circumvention of national laws.

Each of the major existing initiatives to promote financial transparency fails in part to address this problem. The FATF and OECD exercises focus on jurisdictions, not institutions, and create black-lists, but no 'white lists' of jurisdictions that have met the highest standards of best practices. Even if every country and territory in the world were to agree upon their standards, local failures of governmental capacity to regulate or to enforce would preserve the ability of private sector financial institutions who were so inclined to circumvent the standards. The Wolfsberg Principles focus directly on financial institutions, but are limited in scope to private banking, in membership to twelve banks, in principles to basics only, and in enforcement to self-regulation. The Wolfsberg Principles create an implicit 'white list' of subscribing institutions, but without any mechanism for outside audit or assessment, reducing the pressure for comprehensive implementation.

---

[55] The Targeted Financial Sanctions Project of the Watson Institute for International Studies at Brown University, < http://www.WatsonInstitute.org/tfs > contains extensive evidence for this proposition, as a member of the research team on the project, Professor Sue Eckert, has observed.

The foregoing initiatives have been innovative and recent. The question remains whether they will be sufficient, or whether additional mechanisms should be developed that combine their best features into a regime which further attenuates regulatory and enforcement arbitrage, holds the private sector financial services infrastructure accountable, and provides incentives to institutions that adopt best practices.

The World Bank, and the other International Financial Institutions (IFIs) are each among the most important international institutions operating in the world today, controlling many billions of dollars in resources that are, in turn, allocated for lending around the world. These institutions each have a large number of correspondent banking relationships and deposit funds for use in recipient countries, not only in central banks but in commercial ones. Similarly, the United Nations and its constituent elements direct substantial sums in development assistance, which also are necessarily deposited in banks in the countries where the activities are carried out. Trade finance activities undertaken by government-sponsored entities such as export/import banks also rely on private sector banks to handle the funds. National and international development programmes place their funds in private banks. And government and international organizations alike, when they borrow and issue notes, also select international banks to act as agents and issuers.

Today, financial transparency is not a criterion for the selection of one financial institution over another to be the holder, processor, or handler of the funds of governments, development organizations, international financial organizations, or the United Nations. An international bank that is involved in numerous money laundering scandals or terrorist financial transactions has approximately the same chance of obtaining a lucrative source of government resources as does an international bank that has imposed the highest standards of transparency and anti-money laundering policies and procedures. Despite the existence of the FATF, OECD, and Wolfsberg models, there is no 'white list' to which governments, international organizations, or non-governmental organizations that wish to foster transparency can turn as a principled means of selecting a bank to handle their funds.

The lack of such a white list may constitute a missed opportunity. As Robert Litan has observed, these institutions, especially the IFIs, have 'accumulated power akin to a domestic sovereign government', and have the means to enforce terms of their agreements with other countries.[56] With such power in relationship to sovereign states, these institutions surely have equal power should they care to exercise it in relation to private sector institutions. Creating an additional incentive for financial institutions to adhere to a comprehensive, global code of conduct to combat money laundering and protect against illicit finance would seem to be a logical goal for an international community increasingly focused on the risks created by financial

[56] Litan, id, at 199.

secrecy. It would supplement the work of nations by asking institutions that operate in many jurisdictions to adhere to the same standards in all of them, even in cases where the governments themselves have little ability directly to regulate or enforce these standards.

To make a white list system work, the United Nations could, for example, take the recommendations previously made by the FATF, OECD and Wolfsberg Group and ask financial institutions to agree to adopt them on a global basis throughout their institutions. Such institutions could further agree to be assessed by a multinational team of experts who would make reports on the implementation of the principles by those institutions they assess. An institution that has agreed to an assessment and passed it would be credentialed and rewarded with a preference for selection in processing the funds controlled by the UN and by other international organizations. Other, non-white listed institutions would not be denied the opportunity to handle the funds of international organizations. However, they might well be limited to handling such funds in areas where there is no 'white list' institution available. To insure the integrity of the system, the white list would need to be updated regularly, with periodic inspections and reviews of any institution placed on such a list.

Such a system would retain the mutual assessment and oversight elements of the FATF and OECD exercises, while adding the universality promised by the Wolfsberg Principles, and combating the problem of regulatory arbitrage. Each white-listed institution would be required to agree to maintain its know-your-customer and other anti-money laundering policies and procedures regardless of whether it was located in a well-regulated jurisdiction or one with a lax regime. It would accept the principle of having others conduct period external assessments of its compliance with the standards and the publication of comprehensive reports describing how it had met the standards. To ensure fairness and the opportunity to improve anti-money laundering programmes over time, white-listed institutions would be given a period allowing them to correct following each evaluation before being placed at risk of losing white-list status. Other institutions, not white listed, would be given the ability to sign up to the white list at any time by providing a public specification of their methods of complying with the standards, and agreement to submit to an outside assessment at the earliest convenience of the multilateral experts group.

Given the magnitude of the potential commercial benefit to white-listed financial institutions, it would be important to have the standards appropriately tailored by sector, size of operation, and nature of risk. This approach would be similar to that currently undertaken by the Basel Group in the area of risk-based capital standards for financial institutions. To be effective, anti-money laundering regimes need to be structured so as to account for the actual mechanisms by which failures of transparency are most likely to be exploited. Effective tailoring of a white list would require further development of money laundering typologies by the FATF and other organizations. However, even a base-line set of standards, based on those already adopted by the FATF, the OECD, and reflected in the Wolfsberg Principles, might

provide a suitable place to begin. A white-listed institution might still find itself being used to transport terrorist funds. But it would have powerful incentives for preventing such use in the first instance and for swiftly responding to abuses upon discovery incentives that today, with all of the name and shame exercises and the terrible costs of financial crime (including the financing of terrorism) to civilization, nevertheless remain largely absent.