EU NON-PROLIFERATION CONSORTIUM
*The European network of independent non-proliferation think tanks*

NON-PROLIFERATION PAPERS
No. 24 December 2012

# COMBATING PROLIFERATION FINANCING: A EUROPEAN BANKING PERSPECTIVE

INDRANIL GANGULI AND JULIEN ERNOULT*

## I. INTRODUCTION

Since the signing of the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (Non-Proliferation Treaty, NPT) and other international conventions, the threat of global proliferation of nuclear, biological and chemical weapons of mass destruction (WMD) has featured prominently in international politics and relations.[1] In contrast, the financing of WMD proliferation as well as related technologies, goods and services only appeared on the agenda of the United Nations and other international organizations in the wake of the terrorist attacks on the United States of 11 September 2001 and the international disputes over the nuclear armament programmes of Iran and the Democratic People's Republic of Korea (DPRK, or North Korea), with the USA taking a lead role in the international debate and decision-making process.[2]

[1] Noack, P., *Internationale Politik* [International Politics] (Deutscher Taschenbuch Verlag: Munich, 1981), pp. 150–151; Häckel, E., 'Internationale Nuklearpolitik' [International Nuclear Politics], W. Woyke ed., *Handwörterbuch Internationale Politik* [Concise Dictionary of International Politics] (Bundeszentrale für politische Bildung: Bonn, 1986), pp. 227–228; and Bothe, M., 'Friedenssicherung und Kriegsrecht' [Peacekeeping and Martial Law], W. Graf Vitzthum ed., *Völkerrecht* [International Law] (De Gruyter: Berlin, 2010), pp. 688–691. On the NPT and other international conventions see <http://www.un.org/en/globalissues/disarmament/>.

[2] Cordesman, A. H., 'Iran and the United States: the nuclear issue', *Middle East Policy*, vol. 15 (2008), p. 19; and Ganguli, I., *'Smarte' Finanzsanktionen der Europäischen Union als Instrument der Gemeinsamen Außen- und Sicherheitspolitik: Eine Beurteilung der Umsetzungs- bzw. Durchführungseffektivität ausgewählter Maßnahmen aus politikwissenschaftlicher und bankpraktischer Sicht* [The European Union's 'smart' financial sanctions as an instrument of the Common

* The views expressed in this paper are those of the authors and do not necessarily reflect the views of the organizations they are employed by. The contents of the paper are intended for general information purposes only and do not constitute legal advice on any specific facts or circumstances.

## SUMMARY

**The issue of financing the proliferation of weapons of mass destruction (WMD) has gained momentum recently as a result of international disputes over the nuclear armament programmes of Iran and the Democratic People's Republic of Korea. The European Union (EU), as part of wider efforts by the international community, has put in place a complex regime to prevent and combat the financing of WMD proliferation. This regime can be characterized as a new hybrid, with elements borrowed from the conventional financial sanctions and the anti-money laundering/combating the financing of terrorism regimes.**

**This paper addresses the practical implementation difficulties of the EU's anti-proliferation financing regime and the role that the banking sector can play in the fight against WMD proliferation and its financing. It argues that—next to national export control measures aimed at restricting the illicit transfer of proliferation-related goods and services—financial measures can only play a limited role, because banks are not provided with adequately updated and actionable information on proliferators by the competent authorities.**

## ABOUT THE AUTHORS

**Indranil Ganguli (Germany) is an economist and division manager at the Association of German Public Banks (Bundesverband Öffentlicher Banken Deutschlands) in Berlin, where he works on issues relating to banking supervision, anti-money laundering regulations, financial sanctions and foreign trade.**

**Julien Ernoult (France) is Senior Adviser to the Secretary General at the European Association of Public Banks (EAPB) in Brussels, where he works on European and international regulation relating to anti-money laundering, counterterrorism financing and financial sanctions. He holds a degree in European Politics and Governance from the London School of Economics and Political Science.**

Moreover, the recent US Senate probe into the activities of the Hong Kong and Shanghai Banking Corporation (HSBC) and the charges pressed by US regulators against Standard Chartered for allegedly breaching sanctions on Iran have brought the role of the banking sector in fighting financial crime and money laundering, as well as combating the financing of terrorism and proliferation of WMD, to public attention.[3] As a consequence, political decision makers and government authorities now take a greater interest in the actual implementation of financial sanctions as well as the related and interlinked issues of anti-money laundering (AML), combating the financing of terrorism (CFT) and the fight against transnational crime.

The phenomena of money laundering, transnational crime, international terrorism and its financing, and WMD proliferation threaten the legal and democratic order on which the political, social and economic stability of states is based. The international community has therefore responded in various ways to the challenges posed by the constantly changing nature of these threats. With regard to WMD proliferation, the focal issue of this paper, the UN Security Council, the USA and the European Union (EU) have adopted a number of measures that lay the foundations for the emergence of an anti-proliferation financing (APF) regime. Together with the AML and CFT provisions and the financial sanction measures, the EU has in the meantime succeeded in creating three supranational regimes with an impressive array of requisite instruments to address the aforementioned threats and thereby ensure the overarching objective of 'good global governance'.[4] The regimes now in place have, in the opinion of renowned scholars, as well as AML/CFT and sanctions experts, earned the EU wide recognition as a key actor in international politics.[5]

However, the far-reaching, standard-setting competencies of independent agencies operating within supranational and international networks of national regulators on the basis of 'soft' international law and the transposition of such standards into EU law have, to a certain extent, led to a credibility crisis regarding the quality and integrity of EU regulations.[6] This is, in particular, linked to the issue of inadequate coordination of measures between international agencies and national regulators involved in the standard-setting process, and has resulted in highly complex, opaque and, to some extent, contradictory layers of regulation. This regulatory complexity, in turn, makes it extremely difficult, if not impossible, for economic actors such as banks (as addressees of the measures) to effectively implement these measures.

Furthermore, from a foreign and security policy perspective, due consideration should be given to the fact that the requirements setting out the different obligations for banks concerning AML/CFT and financial sanctions have been developed independently of each other and with very distinct objectives and threats in mind. Although the regimes borrow certain elements from (and rely to a certain degree on) each other, they do not constitute a fully integrated or harmonized system of rules and regulations. Instead, they resemble a patchwork of provisions that also harbour potential compliance risks and legal uncertainty for banks. The challenges for banks are further compounded as they are trapped in the dialectics of pursuing their entrepreneurial and economic activities based on legal certainty as an

Foreign and Security Policy: an assessment of the effectiveness of implementation and execution of selected measures from a politological and banking perspective], PhD dissertation, Johann Wolfgang Goethe Universität, Frankfurt, 2012, pp. 172–185.

[3] 'HSBC helped terrorists, Iran, Mexican drug cartels launder money, Senate report says', *Forbes*, 16 July 2012; 'StanChart stunned by force of New York attack', *Financial Times*, 8 Aug. 2012; 'Briten zittern um US-Banklizenz' [British fear losing US banking licence], *Handelsblatt*, 8 Aug. 2012; and 'Standard Chartered schließt Vergleich' [Standard Chartered reaches a settlement], *Frankfurter Allgemeine Zeitung*, 15 Aug. 2012.

[4] Ganguli, I. et al., 'The Third AML Directive: Europe's response to the threat of money laundering and terrorist financing', Parts I–III, *Banking Law Journal,* vol. 126, no. 7 (July/Aug. 2009), pp. 577–601; *Banking Law Journal*, vol. 126, no. 8 (Sep. 2009), pp. 728–759; and *Banking Law Journal,* vol. 126, no. 9 (Oct. 2009), pp. 787–847. See also Ganguli, I., 'The Third Directive: some reflections on Europe's new AML/CFT regime', *Banking and Financial Services Policy Report*, vol. 29, no. 5 (May 2010), pp. 1–18. The concept of 'good global governance' can be defined as the sum of options available to individual persons, institutions, groups, governments and states to interact with each other and discharge tasks that lie in their common interest. The objective of these interactions is to reconcile diverging or conflicting interests of the actors within the framework of a continuous, broad-based, dynamic and complex process by using a cooperative and consensual approach and enabling effective rule through international organizations and international law in a world that is perceived and understood as a 'global neighbourhood'. See Commission on Global Governance, 'Our global neighbourhood', Report, 1991, <http://www.gdrc.org/u-gov/global-neighbourhood/index.htm>, chapter 1, p. 2; and Ganguli (note 2), p. 66.

[5] United States Court of Appeals for the Second Circuit, Rothstein vs. UBS, 09-4108-cv, Brief of *Amici Curiae* the European Banking Federation et al., 28 May 2010, p. 6; and Hufbauer, G. C. and Oegg, B., 'The European Union as an emerging sender of economic sanctions', *Aussenwirtschaft*, vol. 58, no. 4 (2003), p. 547.

[6] Majone, G., 'The credibility crisis of community regulation', *Journal of Common Market Studies*, vol. 38, no. 2 (June 2000), p. 273.

essential socio-economic prerequisite, and of executing their assigned security policy role by complying with the aforementioned patchwork of regime provisions which, due to a lack of clarity and consistency, explicitly fail to deliver legal certainty.[7] These issues have generated a great deal of tension between the financial industry and the government authorities.

Finally, despite the implementation challenges, the banking industry has made considerable progress in complying with the rules and regulations and thereby supports the EU's strategy of combating the aforementioned threats. However, it should also be pointed out that governments worldwide (including in the EU member states) have reacted by consecutively tightening the banking and AML/CFT regimes alongside financial sanctions and APF regime measures.[8] Due to their prominent role as intermediaries and payment service providers in the global financial system, financial institutions have been gradually entrusted with certain investigative functions that had formerly been the exclusive prerogative of police and judicial authorities.[9] These functions expose financial institutions to substantial compliance and legal risks and are associated with considerable administrative and organizational burdens as well as severe fines and criminal penalties.[10]

This paper addresses the practical implementation difficulties and the role that the banking sector can play in the fight against WMD proliferation and its financing. It draws on discussions with representatives of European financial institutions, international organizations, representatives of governments, and competent supervisory, judicial and police authorities from the EU and its member states, as well as academia. It aims to shed some light on the issue of how to make the fight against proliferation more effective from a banking perspective.

Part II provides an overview of the legal and policy framework of the sanctions and the AML/CFT regime. The AML/CFT regime provides the requisite due diligence and research instruments for monitoring customers and for potential detection of their involvement in illicit, terrorist or proliferation financing activities. Part III highlights current international and EU debates on the rationale and objectives of APF measures and how mechanisms and tools of the AML/CFT and financial sanctions regimes could provide added value for APF purposes. It also highlights the linkages and interactions between the provisions of the three regimes that pose significant compliance and economic challenges and risks for banks, as they are charged with preventing their institutions from being abused for illicit purposes and protecting their assets and reputation.[11] Part IV focuses on the lessons learned and the difficulties faced by the banking sector while implementing the provisions of the EU's APF-related sanctions against Iran and North Korea. It also offers some pragmatic policy recommendations from a European banking sector perspective. Part V concludes with a critical review of the sanctions regime of the EU and provides an outlook on future challenges.

## II. THE POLICY AND LEGAL FRAMEWORK

### The EU's financial sanctions and anti-money laundering/combating the financing of terrorism regimes

Although not always obvious at first, the financial sanctions regime of the EU—especially the APF-related measures focusing on Iran and North Korea—is interlinked with a number of other cognate regimes, notably in the areas of AML/CFT and payments and wire transfers.[12] Policymakers and security experts in

[7] Weber, M., *Economy and Society: An Outline of Interpretive Sociology*, eds G. Roth and C. Wittich (University of California Press: Berkeley, 1978), p. 833.

[8] On this issue see Ganguli, 'The Third AML Directive', Part I (note 4), p. 581.

[9] For the purposes of this paper, the term 'financial institution' is interchangeable with 'bank'. However, from a supervisory law perspective, 'financial institution' covers banks, credit institutions, securities companies, insurance providers and other financial service providers pursuant to Article 3, Directive 2005/60/EC of the European Parliament and the Council of 26 Oct. 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *Official Journal of the European Union*, L309, 25 Nov. 2005. The directive is referred to as the Third Anti-Money Laundering Directive or 3AMLD.

[10] Ganguli (note 2), p. 406.

[11] Achtelik, O. and Ganguli, I., 'Geldwäschebekämpfung als Bestandteil des internen Risikomanagements' [Anti-money laundering as part of internal risk management] in *Risikoorientierte Geldwäschebekämpfung* [Risk-based Combat of Money Laundering] (Finanz Colloquium Heidelberg: Heidelberg, 2011), p. 8.

[12] Ganguli, I., *EU-Finanzsanktionen: Eine praxisorientierte Einführung* [Financial Sanctions of the EU: A Practitioner's Guide] (VÖB-Schriftenreihe: Berlin, 2006), pp. 16, 31–33, 57–58; and Graves, R. and Ganguli, I., 'Extraterritorial application of the USA PATRIOT Act and related regimes: issues for European banks operating in the United

the EU need to be aware of the major aspects of, and interactions between, these regimes.

*Implementation of UN-based and autonomous financial sanctions in the EU*

As part of its Common Foreign and Security Policy (CFSP) framework, the EU has adopted several regulations in recent years imposing financial sanctions on both natural and legal persons. The adoption of these regulations corresponds to a paradigm change at the international level since the late 1990s, when the UN and its member states increased their use of targeted financial sanctions—often referred to as 'smart' sanctions, in contrast to traditional, comprehensive economic sanctions—as instruments of 'economic statecraft' due to their selective and focused approach.[13] Initially targeting dictators or governments violating human rights and international law, these restrictive measures play an increasing role in the fight against terrorism or WMD proliferation and their financing. Specifically, the financial sanction resolutions adopted by the UN Security Council pursuant to the provisions of Chapter VII (Articles 39 and 41) in connection with Articles 25 and 48 of the UN Charter represent differentiated, phased and punitive as well as corrective measures of economic statecraft directed against violators of international law and their actions that threaten global peace, security and stability. The measures provide UN member states with instruments that substitute the use of violence or military force and are therefore regarded today as an integral part of the toolbox to ensure peace and other global governance objectives within the UN system of international collective security.[14]

The measures of the Council of the EU have been mostly adopted within the framework of the CFSP and on the basis of international law, including various UN Security Council resolutions as well as Articles 25–41 of the Treaty on European Union (TEU) in connection with Articles 215, 288–292 and 352 of the Treaty on the Functioning of the European Union (TFEU).[15] Pursuant to Article 288 of the TFEU, all regulations of the sanctions regime, including those against the financing of terrorism (the so-called anti-terrorism and Al-Qaeda regulations) and against WMD proliferation financing (currently, the so-called Iran and North Korea regulations) are binding in their entirety and directly applicable in all EU member states, thus taking precedence over national laws.[16]

The regulations include a number of components and characteristics that are essential to the design of a 'smart' financial sanctions regime.

States', *Privacy and Data Security Law Journal*, vol. 2, no. 11 (Oct. 2007), pp. 968, 996.

[13] Cortright, D. and Lopez, G. A., (eds), *The Sanctions Decade: Assessing UN Strategies in the 1990s* (Lynne Reinner Publishers: Boulder, CO, 2000); Cortright, D. et al., 'Targeted financial sanctions: smart sanctions that do work', eds D. Cortright and G. A. Lopez, *Smart Sanctions: Targeting Economic Statecraft* (Rowman & Littlefield: Lanham, MD, 2002); and Ganguli (note 2), pp. 49, 71.

[14] Brock, L., 'The United Nations: forum for "one world"?', eds W. Hoppenstedt, Pruessen, R. and Rathkolb, O., *Global Management* (LIT Verlag: Vienna, 2005), p. 53; Brock, L., 'The use of force in the post-cold war era: from collective action back to pre-charter self-defense?', eds M. Bothe, M. E. O'Connell and N. Ronzitti, *Redefining Sovereignty: the Use of Force after the Cold War* (Transnational: Ardsley, NY, 2005), p. 27; Bothe (note 1), pp. 645–690; and Ganguli (note 2), pp. 23–28.

[15] Consolidated Version of the Treaty on European Union, *Official Journal of the European Union*, C115, 9 May 2008, p. 13; Consolidated Version of the Treaty on the Functioning of the European Union, *Official Journal of the European Union*, C115, 9 May 2008, p. 47. See also Kreutz, J., *Hard Measures by a Soft Power? Sanctions Policy of the European Union*, Bonn International Centre for Conversion (BICC) Paper no. 45 (BICC: Bonn, 2005), p. 11; Ganguli (note 2), pp. 122–129, 132; Achtelik and Ganguli (note 11), p. 8; and Ganguli (note 12), p. 15. It should be noted that the EU has also adopted autonomous—that is, non-UN Security Council—sanctions, e.g. Council Regulation (EC) no. 314/2004 of 19 Feb. 2004 concerning certain restrictive measures in respect of Zimbabwe, *Official Journal of the European Union*, L55, 24 Feb. 2004 and Council Regulation (EC) no. 765/2006 of 18 May 2006 concerning restrictive measures against President Lukashenko and certain officials of Belarus, *Official Journal of the European Union*, L134, 20 May 2006.

[16] On the anti-terrorism regulation see Council Regulation (EC) no. 2580/2001 of 27 Dec. 2001, *Official Journal of the European Communities*, L344, 28 Dec. 2001, p. 70. This regulation was adopted on the basis of UN Security Council Resolution 1373, 28 Sep. 2001. On Al-Qaeda see Council Regulation (EC) no. 881/2002 of 27 May 2002, *Official Journal of the European Communities*, L139, 29 May 2002, p. 9. This regulation was adopted and, concerning material aspects, further amended on the basis of UN Security Council Resolution 1267, 15 Oct. 1999; UN Security Council Resolution 1333, 19 Dec. 2000; UN Security Council Resolution 1390, 28 Jan. 2002; UN Security Council Resolution 1452, 20 Dec. 2002; UN Security Council Resolution 1988, 17 June 2011; and UN Security Council Resolution 1989, 17 June 2011. On Iran see Council Regulation (EC) no. 423/2007 of 19 Apr. 2007, *Official Journal of the European Union*, L103, 20 Apr. 2007, repealed by Council Regulation (EC) 961/2010 of 25 Oct. 2010, *Official Journal of the European Union*, L281, 27 Oct. 2010, repealed by Council Regulation (EU) 267/2012 of 23 Mar. 2012, *Official Journal of the European Union*, L88, 24 Mar. 2012, p. 1. The regulations concerning Iran were adopted on the basis of UN Security Council Resolution 1737, 23 Dec. 2006; UN Security Council Resolution 1747, 24 Mar. 2007; and UN Security Council Resolution 1803, 3 Mar. 2008. On North Korea see Council Regulation (EC) no. 329/2007 of 27 Mar. 2007, *Official Journal of the European Union*, L88, 29 Mar. 2007, p. 1. This regulation was adopted and, concerning material aspects, further amended on the basis of UN Security Council Resolution 1718, 14 Oct. 2006; and UN Security Council Resolution 1874, 12 June 2009.

1. Orders to freeze the funds, financial assets and economic resources of listed (natural and legal) persons and entities.
2. Prohibitions on making funds and economic resources available.
3. Prohibitions on circumventing the restrictive measures.
4. Exemptions from the freezing of funds and the prohibition on making funds and economic resources available (e.g. allowing the deduction of fees for routine holding or maintenance of frozen funds or economic resources of listed persons and additions of interest and other earnings as well as incoming payments and the subsequent freezing of such additions).
5. Official authorization procedures to release frozen funds and economic resources.
6. Reporting obligations to competent authorities.
7. Exemptions from liability (indemnity in case of erroneously frozen assets) for financial institutions and other addressees of the measures.[17]

The objective of the targeted measures is not simply to freeze the assets of listed persons and entities but, more importantly, to prevent them from having direct access to their funds and other economic resources in the EU. The nearly 30 regulations of the regime contain, in their respective annexes, comprehensive lists of natural and legal persons as well as other entities subject to the restrictive measures. Currently a total of approximately 5 000 persons or entities are listed on the website of the EU's European External Action Service (EEAS).[18] According to renowned scholars and experts, the evolution of the EU's smart sanctions regime has made it an emerging and powerful 'sender' of financial and economic sanctions.[19]

However, the financial sanctions regime of the EU has been subject to much controversial debate due to inherent legal inconsistencies between the regulations. Examples of inconsistencies that exist between the modern and older generations of EU regulations (especially the CFT-related sanctions) include (*a*) differing definitions of the terms 'money', 'resources' and 'financial services'; and (*b*) the differing scope of the provisions governing asset freeze, non-availability of funds, authorization and exemption procedures, as well as liability of addressees in case of an erroneous freezing of assets of innocent customers[20]

Moreover, the lack of proper listing and delisting procedures ensuring the protection of fundamental human rights (e.g. the right to respect for property, the right to be heard and the right to effective judicial review, including redress in case of wrongful listings) has invited severe criticism from experts and the European Court of Justice (ECJ), which issued landmark rulings in 2008 that led to revisions of numerous regulations of the financial sanctions regime.[21] These inconsistencies are also largely responsible for the aforementioned legal uncertainty and considerable compliance risks which banks face when implementing and executing the provisions.

### *The Third EU Anti-Money Laundering Directive and related regulations*

The issues of money laundering and terrorist financing provide useful insights into, and analogies to, methods and patterns of covert or clandestine proliferation financing operations that are difficult to detect from a banking perspective. The AML/CFT regime provides the requisite due diligence, research and analytical tools for monitoring customers and detecting patterns of illicit activity that may have a terrorist or proliferation financing background.

While, from an analytical point of view, money laundering and terrorist financing pursue fundamentally different objectives, it is widely

[17] Ganguli, 'The Third AML Directive', Part III (note 4), p. 795–796.
[18] European External Action Service, 'Consolidated list of persons, groups and entities subject to EU financial sanctions', 6 Nov. 2012, <http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm>.
[19] Hufbauer and Oegg (note 5), p. 547.
[20] For a thorough review of this issue see Ganguli (note 2), p. 376–414.
[21] Joined Cases C-402/05 P and C-415/05 P: Judgment of the Court (Grand Chamber) of 3 Sep. 2008, 2008/C 285/03, *Official Journal of the European Union*, C285, 8. Nov. 2008, p. 2. See also Herzog, F., 'Einleitung' [Introduction], ed. F. Herzog, *Geldwäschegesetz (GwG): Kommentar* [The Anti-Money Laundering Act (AMLA): A Commentary] (C. H. Beck: Munich, 2010), pp. 61–63; Tzanakopoulos, A., *Disobeying the Security Council: Countermeasures against Wrongful Sanctions* (Oxford University Press: Oxford, 2011), p. 150; Goldirova, R., 'EU terror blacklist suffers judicial blow', EU Observer, 4 Sep. 2008, <http://euobserver.com/9/26685>; Brock, L., 'Von der liberalen Universalpoesie zu reflexiver Friedenspolitik! Die Demokratie als Medium einer brisanten Vermittlung zwischen Frieden und Gerechtigkeit' [From liberal universal thought to reflective peace policy! Democracy as a medium for a politically sensitive interaction between peace and justice], eds C. Baumgart-Ochse et al., *Auf dem Weg zu Just Peace Governance: Beiträge zum Auftakt des neuen Forschungsprogramms der HSFK* [On the Path to Just Peace Governance: Contributions for the Inception of the New Research Programme of the PRIF] (Nomos: Baden-Baden, 2011), p. 47; and Ganguli (note 2), p. 251.

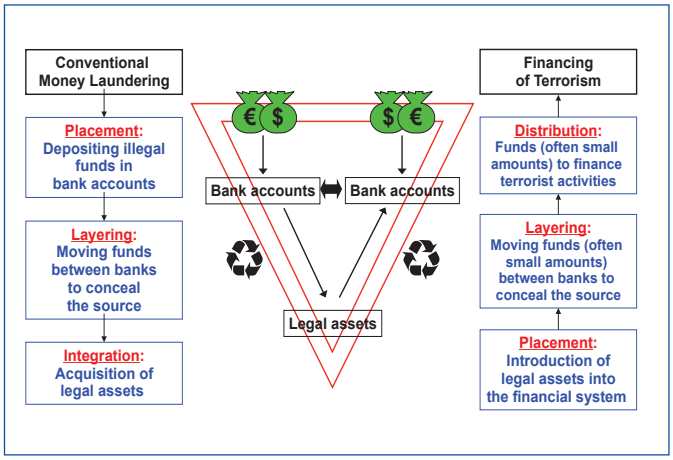


**Figure 1.** Three-phase model of money laundering and terrorist financing

*Sources*: Adapted from Ganguli, I., *EU-Finanzsanktionen: Eine praxisorientierte Einführung* [Financial Sanctions of the EU: A Practitioner's Guide] (VÖB-Schriftenreihe: Berlin, 2006), p. 32; and International Monetary Fund (IMF), *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (IMF: Washington, DC, 2004), p. 8.

recognized that strong links do exist between the two phenomena (see figure 1).[22]

The proceeds of criminal activities such as drug trafficking are generally collected by criminal individuals or organizations in the form of cash and then laundered by depositing or 'placing' the incriminated funds in bank accounts, often below the legally stipulated monetary thresholds in order to avoid customer due diligence (CDD) and the internal control procedures established by banks. In order to give their operations and transactions a veneer of legality and to conceal the illicit source, money launderers can move the incriminated funds between various bank accounts within a country or in different jurisdictions by employing 'layering' techniques. Thereafter they often acquire legal assets (e.g. real estate) in order to 'integrate' the assets and clean up the paper trail.

Terrorist financing differs from money laundering because the thrust of the operations is in the opposite direction. The funds—often derived from legitimate sources or persons who may not appear to be associated with terrorism—are, with the help of the same layering techniques as conventional money laundering, moved through bank accounts before being distributed to different beneficiaries (often in small amounts) for illegal purposes (e.g. to finance terrorist activities). These patterns and interdependencies between money laundering and terrorist financing as well as the resulting business, operational and reputational risks have caused financial institutions to employ analytical and electronic data processing (EDP) tools developed for AML purposes in order to combat the financing of terrorism. However, the results of detecting terrorist financing activities have not been very good, as the beneficiaries of such terrorist funds are generally not customers of the bank from which the originator (with a legitimate background) authorized a money transfer and are, therefore, not identifiable for CFT purposes. Further, a bank may not, despite rigorous application of CDD measures and EDP research tools, be in a position to detect that one of its customers with a legitimate business background and accounts is potentially involved in terrorist financing activities.

Terrorist financing and proliferation financing share some procedural characteristics, as the funds supporting proliferation emanate primarily from government coffers or legitimate businesses. Therefore, regulators often believe that the same research tools can, to some extent, be used for the detection of proliferation financing patterns too. Indeed, it can be reasonably assumed that financers of proliferation—although possibly using more sophisticated commercial transaction channels and instruments—would employ similar placement, layering and distribution techniques for their funds in order to conceal the procurement process and the final use of WMD proliferation related technology and to clean up the paper trail.[23] As in the case of terrorist financing, the beneficiaries (or end users) of proliferation-related funds are in most cases not customers of, and therefore unknown to, the bank of the originator of the wire transfer. Only the bank of the beneficiary of such funds may have some insight into the proliferation-related financing activities of its customer. This is one of the major reasons why banks and other financial institutions find it extremely

[22] International Monetary Fund (IMF), *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (IMF: Washington, DC, 2004), p. 1–5; Ganguli (note 12), p. 31; and Ganguli, I., 'Neue Geldwäsche-Richtlinie: Erste Bewertung aus Bankensicht' [New money laundering directive: an initial assessment from a banking perspective], *BankPraktiker*, issue no. 02/2006, p. 74.

[23] Ben Ouagrham-Gormley, S., 'Banking on nonproliferation', *The Nonproliferation Review*, vol. 19, no. 2 (2012), p. 248; and Ganguli, I., 'FATF-Leitlinien zur Bekämpfung der Proliferationsfinanzierung: Eine Einschätzung aus bankenpraktischer Sicht' [FATF guidance on the combat of proliferation financing: an assessment from a practitioner's perspective], *BankPraktiker*, issue no. 12/2007, pp. 622–626.

difficult, if not impossible, to detect proliferation financing activities.[24]

Against this backdrop and given the threat of rapidly spreading networks of transnational crime since the 1980s, the original impulse to create an international framework for the fight against money laundering originated with the UN, its Security Council and specialized agencies as well as other international bodies like the Financial Action Task Force on Money Laundering (FATF) founded in 1989.[25] The FATF first published its AML standards—the FATF 40 Recommendations (FATF 40)—in 1990 and has subsequently revised them over time (most recently in February 2012) in order to include CFT and APF standards within their scope.[26] Although the FATF 40 are strictly speaking 'soft' law they are recognized as the international benchmark in the area of AML/CFT/APF today.

The EU and its member states supported these international initiatives and therefore regarded the legislation of measures at the supranational level as essential to the success of AML/CFT efforts. These considerations culminated in the Third Anti-Money Laundering Directive (3AMLD), which entered into force on 15 December 2005.[27] The structural changes brought about by the 3AMLD legislation were vast and represented a quantum leap in the evolution of the EU's AML/CFT regime compared with the previous two directives.[28] The scope of predicate offences and criminal activities (e.g. drug/narcotics trafficking or offences punishable by deprivation of liberty or a detention order) covered by the 3AMLD is very broad. It covers generating proceeds from serious crime, participation in criminal organizations and terrorist financing activities. Salient features of the 3AMLD are as follows.[29]

A key component is the introduction of the risk-based approach (RBA), which constitutes a completely new method with far-reaching consequences for the practical implementation of AML/CFT rules and requirements by financial institutions. The RBA breaks with the very formal and inflexible methods propagated by the rule-based approach, which did not leave any room for a risk-sensitive differentiation in the application of measures. Pursuant to the RBA, financial institutions in the EU are required to distinguish between low, medium and high categories of risk within the framework of banks' CDD process and Know Your Customer (KYC) policies. This is to be done: (*a*) when establishing a business relationship (account-based); (*b*) upon execution of transactions outside an established business relationship (occasional non-account based transactions) amounting to €15 000 or more; (*c*) in case of suspicion of money laundering or terrorist financing, regardless of any exemption or threshold; or (*d*) if there are doubts about the veracity or adequacy of previously obtained customer identification data.

Accordingly, financial institutions are obliged to apply at least the following three degrees of CDD measures.

1. *Simplified CDD*. Pursuant to Articles 11–13 of the 3AMLD, banks are allowed to bypass general CDD measures regarding customers (e.g. other financial institutions, public authorities and stock exchange listed companies in EU member states or equivalent third country jurisdictions) and products (e.g. life insurance policies and pension plans) representing low risks.

2. *General CDD*. Pursuant to Articles 7–10, banks are required with regard to customers representing medium risks to (*a*) identify their customers (natural and legal persons); (*b*) identify, where applicable, the beneficial owners (BOs) of customers (i.e. natural persons controlling more than 25 per cent of the shares

[24] These views were recently confirmed by a panel of experts at an AML/CFT/APF conference in Potsdam, Germany (12–14 Sep. 2012), including Alexander Freiherr von Hardenberg, currently deputy head of an AML compliance group at one of Germany's large and internationally active banks.

[25] For further details concerning the Financial Action Task Force on Money Laundering (FATF) see <http://www.fatf-gafi.org>; Herzog (note 21), p. 63; Ganguli, 'The Third AML Directive', Part I (note 4) p. 582; and Achtelik and Ganguli (note 11), p. 8.

[26] FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, Feb. 2012, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20(approved%20February%202012)%20reprint%20May%202012%20web%20version.pdf>; and Achtelik, O., 'Politisch exponierte Personen in der Geldwäschebekämpfung' [Politically exposed persons in the combat against money laundering], Dissertation, University of Bremen, 2009, p. 51.

[27] Directive 2005/60/EC (note 9), Article 46. The 3AMLD and related legislation are currently being reviewed by the European Commission with a view to incorporating the latest FATF 40 amendments.

[28] For an overview of the evolution of the 3AMLD regime see Ernoult, J., Hemetsberger, W. and Wengler, C., *European Banking and Financial Services Law*, Third Edition (Larcier: Brussels, 2008), pp. 207–213.

[29] Ganguli (note 22) p. 75; and Ganguli, 'The Third AML Directive', Part I (note 4) pp. 585–592.

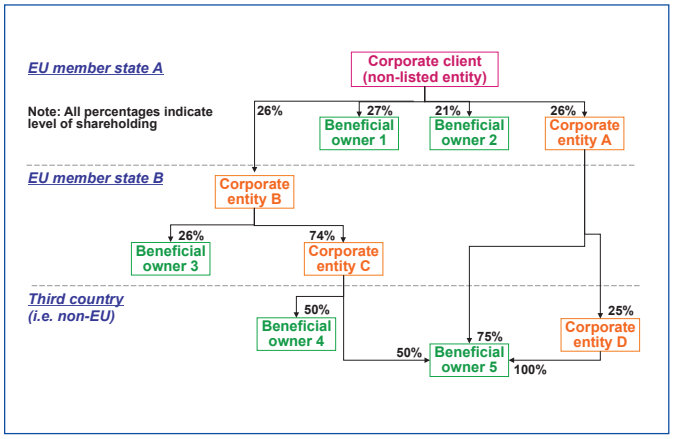


**Figure 2.** Risk-based beneficial owner identification

*Source*: Ganguli, I., 'The Third Directive: some reflections on Europe's new AML/CFT regime', *Banking and Financial Services Policy Report*, vol. 29, no. 5 (May 2010), p. 5.

of a legal entity); (*c*) obtain information on the purpose or intended nature of the business relationship; and (*d*) conduct ongoing monitoring of the business relationship and transactions.30

3. *Enhanced CDD.* Pursuant to Recitals 24–26, Article 3, Paragraph 8 and Article 13, banks are obliged with regard to situations and customers representing high risks (e.g. politically exposed persons, customers physically absent for identification purposes and cross-border correspondent banking relationships with financial institutions from third countries) to apply additional CDD measures such as establishing the source of the customers' funds, obtaining senior management approval before entering a business relationship with such customers and enhanced account monitoring.

If a financial institution is unable to comply with certain key CDD obligations mentioned above, it could refuse to carry out the transaction or even terminate the business relationship. Furthermore, pursuant to Article 22, financial institutions have to consider filing a Suspicious Transaction Report (STR) in relation to the relevant customer with the Financial Intelligence Unit (FIU).

Other important measures from a banking perspective include: (*a*) the prohibition of offering anonymous accounts or products (Article 6) and entering into or maintaining business relationships with 'shell banks' (Article 3, Paragraph 10 and Article 13, Paragraph 5); (*b*) the establishment of internal control, risk assessment, risk management, compliance management and communication of CDD policies and procedures that have to be observed on a group-wide and cross-border basis (Recital 35 and Articles 31–34); and (*c*) appropriate training and information dissemination measures for relevant employees of the banks (Article 35).

Of the CDD requirements imposed by the 3AMLD, one of the most interesting aspects from an APF point of view, but most challenging to implement from a banking perspective, is the KYC-driven obligation of risk-based identification of a customer's BO.[31] Article 3, Paragraph 6 defines the BO as the 'natural person(s) who ultimately own(s) or control(s) the customer and/or the natural person on whose behalf a transaction or activity is being conducted'. In cases of direct ownership, it is usually possible to comply with the CDD obligations in respect of the BO by determining and recording the identity of those natural persons with a shareholding exceeding the 25 per cent threshold. In most cases this can be achieved through a simple enquiry with the customer, company register or commercial register. The obligation, however, may be far more difficult to comply with in cases where one or more intermediate companies (located in different jurisdictions) exist between the customer and the potential BO in the background (see figure 2).

In figure 2 the financial institution would be required to identify BOs 1, 4 and 5 as they either control more than 25 per cent of the customer's shares directly or control 50 per cent or more of the customer's shares indirectly (i.e. through intermediate majority shareholdings from a company law perspective).[32]

[30] The 25 per cent threshold is a minimum legal standard pursuant to Article 3, Paragraph 6 of the 3AMLD. Nevertheless, a bank has the option to identify beneficial owners (BOs) below the threshold if it perceives a customer to be a high-risk client.

[31] See Ganguli, 'The Third AML Directive', Part II (note 4), pp. 733–741.

[32] This method of identifying controlling interest in an intermediate company from a company law perspective by applying, among other things, the 'more than 50%' criterion is recommended in joint guidance from the ministry of finance (Bundesfinanzministerium, BMF), the banking supervisory authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) and the German banking industry (Die Deutsche Kreditwirtschaft, DK) in Germany. See DK, Auslegungs- und Anwendungshinweise der DK zur Verhinderung von Geldwäsche Terrorismusfinanzierung und „sonstigen strafbaren Handlungen [Interpretation and implementation guidelines of the DK for the prevention of money laundering, terrorism financing and other punishable offences], Berlin, 16 Dec. 2011, <http://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_rs_1201_gw_anlage1_AuAs.pdf?__blob=publicationFile&v=6>. The precise method of identification, however, might differ from member state to member state.

From a proliferation financing perspective, it would be prudent to subject these BOs as well as the intermediate corporate entities A–D directly or indirectly controlled by them to further scrutiny and intrusive review in order to find out whether the potential corporate customer is in fact acting as a front company to procure proliferation goods and technology. However, for a financial institution to undertake such a review would be a daunting task, as it is very likely that the potential customer wishing to enter into a business relationship with the bank would not even know whether its beneficial owners located beyond the immediate level of shareholding (and possibly in different jurisdictions) exist and whether they are involved in proliferation-related activities. Therefore, the chances of detecting and identifying BO 5, who in figure 2 appears to be in charge of the whole structure and is domiciled in a third country jurisdiction (possibly a fragile or failed state), as a potential terrorist or proliferation financer are slim if not close to nil.

Finally, mention must be made of the Wire Transfer Regulation, which was adopted by the EU on 7 November 2006 and which transposes the former FATF Special Recommendation VII on wire transfers, including the corresponding interpretative note, into EU law.[33] The regulation aims to combat money laundering and the financing of terrorism by requiring Payment Service Providers (also banks), among other things, to (*a*) conduct CDD checks for transactions over €1000; (*b*) monitor, ongoing and regardless of the amount, information on the originator accompanying incoming payments; and (*c*) inform the relevant authorities of any payments suspected of having a criminal or terrorist background. It is recognized by European supervisors and the banking industry as an important component of a wider framework of regimes.[34] The regulation also shares the 3AMLD's risk-based approach by recognizing the existence of low and high-risk situations in the area of wire transfers that may warrant the application of simplified or enhanced due diligence (pursuant to Recitals 9 and 16). Articles 8–11 of the Wire Transfer Regulation refer to the core obligations of the Payment Service Provider of the payee and, among other things, cover: (*a*) detection of missing information on the payer; (*b*) procedures for the treatment of funds transfers with missing or incomplete information on the payer; (*c*) risk-based assessment of funds transfers with missing or incomplete information on the payer for reporting purposes; and (*d*) record keeping.

Articles 8 and 9 of the Wire Transfer Regulation have given rise to considerable tensions between European regulators and the banking industry within the EU as to the uniform interpretation and implementation of obligations. Obligations of analysis and request regarding missing or incomplete data on the originator in the messages accompanying payments are seen as overly complicated. Many EU banks receive large numbers of wire transfers with incomplete information, in particular from low-risk jurisdictions such as the USA and other major Western economies, making it difficult to screen and process the large volume of payments for completeness of information in real time. Moreover, there is a lack of regulatory guidance to handle the complex patchwork and interplay of provisions, with obligations arising from both the 3AMLD and the EU's financial sanctions regime. Notably, the provisions of the financial sanctions measures against international terrorism, the Taliban and Al-Qaeda (Article 9, Paragraph 1) were also subject to controversial debate between the financial sector and the regulators. Against this backdrop, banking, insurance and securities regulators of the EU member states adopted a Common Understanding in October 2008 to address some of the most critical issues concerning the implementation of Articles 8 and 9.[35] However, unsurprisingly, the guidance did not solve all of the implementation problems. Therefore, it remains to be seen whether the Wire Transfer Regulation will achieve its objectives within the wider framework of regimes, as it also plays an important role in the EU's APF-related sanctions against Iran and North Korea.

[33] Regulation no. 1781/2006 of the European Parliament and the Council of the European Union, 15 Nov. 2006, *Official Journal of the European Union*, L345, 8 Dec. 2006 (known as the Wire Transfer Regulation). Unless otherwise indicated, the following analysis is based on the works of Ganguli, 'The Third AML Directive', Part III (note 4), pp. 788–794; and Ganguli, 'The Third Directive' (note 4), pp. 9–10. The old Special Recommendation VII has been transposed into Recommendation 16 of the revised FATF 40, which now requires the control of information on the beneficiaries of wire transfers.

[34] CEBS/CEIOPS/CESR, Common understanding of the obligations imposed by European Regulation 781/2006, 16 Oct. 2008, <http://www.eba.europa.eu/getdoc/64c0be05-9e6e-44b5-a8de-da6a2ba6813e/2008-16-10-AMLTF-Common-understanding-on-payment-f.aspx>, pp. 1–21.

[35] CEBS 2008 (note 34), pp. 2, 4–15.

## III. ANTI-PROLIFERATION FINANCING: A THIRD PILLAR?

The threat of WMD proliferation and its financing led the UN Security Council to adopt Resolution 1540 on 28 April 2004 and thus lay the foundation for the emergence of an APF regime.[36] The resolution represents a global (as opposed to targeted) approach to the issue and imposes binding obligations on all states to adopt legislation to prevent the proliferation of nuclear, chemical and biological weapons, and their means of delivery by non-state actors, and establish appropriate domestic controls over related materials to prevent their trafficking.[37] The issue of WMD proliferation and its financing has gained further momentum in recent years as a result of the dispute over the nuclear policies and programmes of Iran and North Korea. The US Government has exerted substantial diplomatic pressure on other nations as well as international organizations to effectively thwart the efforts of the Iranian and North Korean governments to acquire nuclear weapon production capability and related technologies.[38] The US efforts resulted in the adoption of UN Security Council Resolution 1718 against North Korea and Resolution 1737 against Iran.[39] These resolutions have created a new hybrid APF and AML/CFT sanctions regime, with significant implications for the role that financial institutions are required to play.

### The Financial Action Task Force's policy and recommendations for combating proliferation financing

The targeted UN Security Council resolutions concerning North Korea and Iran provided the FATF with the legal justification and basis to adopt the Guidance on implementing financial provisions of UN Security Council Resolutions to counter proliferation of weapons of mass destruction (FATF Guidance) at the end of June 2007.[40] The FATF Guidance explicitly refers to UN Security Council Resolution 1737 against Iran.[41] It also contains an appraisal of the closely related regimes of smart sanctions, AML/CFT, banking supervision and foreign trade law as well as recommendations to be considered by banks or financial institutions when implementing activity-based financial prohibitions pursuant to Paragraph 6 of Resolution 1737.[42] Moreover, the FATF published its Additional Guidance in October 2007 that substantiates and tightens the obligations of banks as set forth in the FATF Guidance.[43] Politically, the measure was further reinforced by a FATF statement in which Iran's AML/CFT regime and policy were criticized for being deficient and in which banks in FATF member states were required to observe enhanced CDD with regard to transactions with Iran.[44] In April 2010 the FATF published a status

[36] Later the UN Security Council adopted Resolution 1673 of 27 Apr. 2006 to further intensify its efforts in the field of anti-proliferation financing.

[37] The German Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) defines proliferation as the 'Spread of weapons of mass destruction and/or of products used for producing them, including the required know-how as well as of respective weapon carrier systems'. BfV, 'Proliferation: Wir haben Verantwortung' [Proliferation: we bear responsibility], Köln 2010, <http://www.verfassungsschutz.de/download/SHOW/broschuere_1011_proliferation.pdf>, p. 3.

[38] For a thorough analysis of the US foreign policy response to the perceived threat see Dueck, C. and Takeyeh, R., 'Iran's nuclear challenge', *Political Science Quarterly*, vol. 122, no. 2 (summer 2007), p. 189; Hemmer, C., 'Responding to a nuclear Iran', *Parameters*, vol. 37, no. 2, (autumn 2007), p. 42; and Speier, R., 'Missile nonproliferation and missile defense: fitting them together', *Arms Control Today*, vol. 37, no. 9 (Nov. 2007), p. 15.

[39] UN Security Council Resolution 1718, 14 Oct. 2006; and UN Security Council Resolution 1737, 23 Dec. 2006.

[40] Financial Action Task Force (FATF), 'Guidance on implementing financial provisions of UN Security Council Resolutions to counter proliferation of weapons of mass destruction', 29 June 2007, < http://www.fatf-gafi.org/topics/financingofproliferation/documents/guidanceonimplementingfinancialprovisionsofunsecuritycouncilresolutionstocounterproliferationofweaponsofmassdestruction.html>.

[41] FATF (note 40), Paragraph 1.

[42] FATF (note 40), Paragraphs 17-32.

[43] FATF, 'Guidance regarding the implementation of activity-based financial prohibitions of UN Security Council Resolution 1737', 12 Oct. 2007, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/FATF%20Guidance%20regarding%20the%20implementation%20of%20activity-based%20financial%20prohibitions%20of%20UNSC%201737%202012%20COVER.pdf>.

[44] FATF, Statement on Iran, 11 Oct. 2007, <http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_0708_gw_fatfErklaerung.html>. Since then the FATF has regularly issued such statements on Iran within the framework of its International Co-operation Review Group (ICRG), with the latest public statement issued on 22 June 2012. FATF, 'High-risk and non-cooperative jurisdictions', FATF Public Statement, 22 June 2012, <http://www.fatf-gafi.org/media/fatf/documents/FATF Public statement 22 June 2012.pdf>. FATF statements are communicated to financial institutions operating in the EU through circulars issued by the competent supervisory authorities

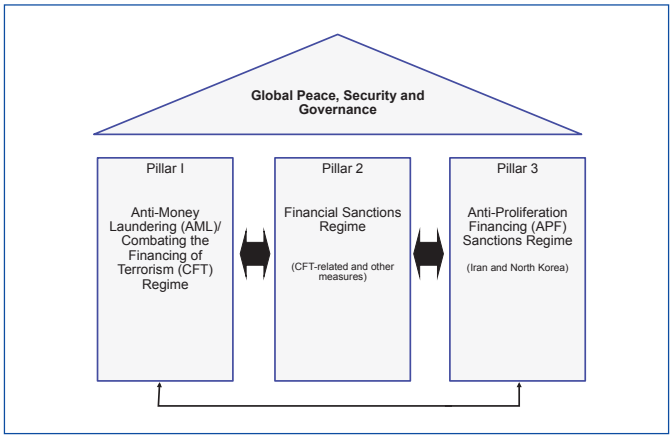


**Figure 3.** The three regime pillars

*Source*: Adapted from various presentations by Ganguli, I. and Ernoult, J.

report on the policy work and consultation being undertaken in relation to proliferation financing.[45] The report calls for states to encourage financial institutions to incorporate the risk of proliferation financing into their established preventive measures and internal controls using a RBA and according to key risk factors.[46] The idea of having risk-based monitoring systems in place has been discussed in several other reports and the FATF Guidance itself, but public authorities have so far failed to tell banks exactly what and whom to look for—as proliferators covertly operating within complex corporate structures and procurement and financing chains are not easily identifiable (see figures 1 and 2).

After the last review of the FATF 40 in 2012, elements of the APF-related guidance have been incorporated into the new Recommendation 7 of the revised FATF 40 and a very detailed Interpretive Note to Recommendation 7 (INR 7).[47] It is therefore reasonable to argue that the FATF's guidance documents together with the FATF 40's Recommendation 7 and INR 7 today constitute a third regime pillar—combating the financing of proliferation or APF—to ensure the objectives of global peace, security and governance. The entire architecture of the AML/CFT, financial sanctions and APF regimes is depicted in figure 3.

Interestingly, the FATF does not refer to the global APF approach of UN Security Council Resolution 1540 in Recommendation 7, but instead promotes the strategy of targeted APF-related sanctions pursuant to Resolution 1718, Resolution 1737 and subsequent resolutions. By doing so, the FATF has decided to pursue a pragmatic policy. This shift might have been influenced by the realization that the global scope of Resolution 1540 is too expansive and does not provide governments and financial institutions with appropriate and actionable instruments to deal with the challenge of detecting the financial flows of unidentified non-state actors involved in WMD proliferation activities. However, the targeted sanctions approach of the third pillar, with its extended scope, has added a further and rather formidable layer of regulatory complexity and opacity, which poses serious implementation challenges for banks.

A closer look at the FATF Additional Guidance reveals that the requirements substantiate and strengthen obligations pursuant to Paragraph 6 of Resolution 1737 in the following areas in particular.

1. The application of enhanced CDD regarding proliferation-related, high-risk customers, products and forms of transactions.[48]

2. The provision of typologies by authorities and the exchange of information between authorities and banks on proliferation-related, high-risk customers and their transactions in order to, among other things, analyse transactional details (also with regard to end users of particular concern) and identify the supply/ delivery channels and possible diversion of items,

[45] FATF, 'Combating proliferation financing: a status report on policy development and consultation', FATF Report, Feb. 2010, <http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf>.

[46] FATF (note 45), see in particular Annex 3.

[47] FATF, 'International standards on combating money laundering and the financing of terrorism & proliferation: the FATF recommendations' <http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html>. Recommendation 7 explicitly requires that 'Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations'. See also Interpretive Note to Recommendation 7, 'Targeted Financial Sanctions Related to Proliferation', pp. 47–53.

[48] Such customers may include, among others, importers, exporters and intermediaries that, due to their participation in prohibited activities pursuant to Paragraph 6 of Resolution 1737, are classified as high-risk customers. Such products are documentary credits, documentary collections, credit lines and loans as well as wire transfers and other financial services. See FATF (note 43), Paragraph 7(d), (e).

materials, equipment, goods and technology sanctioned under Paragraph 6 of Resolution 1737.[49]

3. The development of so-called 'red flag' indicators for detecting possible proliferation contexts and monitoring transactions on the basis of those indicators.[50]

4. Banks' awareness of the risks associated with the use of their correspondent bank relationships in providing financial services or products to high-risk customers or otherwise engaging in high-risk transactions.[51]

On a critical note, the concepts presented by the FATF are based on incorrect and unrealistic assumptions and do not, therefore, provide a suitable basis for clearly distinguishing between high-risk and low-risk customers, transactions and products. Due to the complexity of the issue, the requirements of the FATF Guidance, with its focus on an activity-based approach, are impossible or—at best—extremely difficult for financial institutions to implement. Internationally active banks, in particular, are confronted with a range of multi-jurisdictional compliance and risk management issues as well as structural problems when implementing the guidance.[52] However, the FATF has subsequently realized this problem and modified its approach accordingly in the revised FATF 40. It now focuses on entity-based, as opposed to activity- or goods-based, targeted financial sanctions as the principal instrument in enforcing APF measures.[53]

### EU strategy and measures against proliferation financing

The EU accorded high priority to the issue of WMD proliferation as early as 2003, within the context of the EU Strategy against Proliferation of Weapons of Mass Destruction (WMD Strategy).[54] To that end, the EU has integrated WMD non-proliferation concerns into its political, diplomatic and economic activities and programmes as well as its CFSP strategy. It has also sought to foster dialogue with the industry as one of the key axes of its response to the threat of WMD proliferation. Joining further international efforts to design new measures against proliferation, in December 2008 the Council of the EU adopted New Lines for Action (NLA) in combating the proliferation of WMD and their delivery systems, as a follow up to its 2003 WMD Strategy. The NLA are not intended to replace the WMD Strategy, but rather to make the priorities more operational and provide an increasing role for financial institutions as key partners in the fight against proliferation.[55] The document states that the EU is determined to (*a*) intensify its efforts to counter proliferation flows and proliferation financing; (*b*) raise awareness in financial institutions and undertakings and scientific and academic circles; (*c*) impose sanctions on acts of proliferation; and (*d*) develop measures to prevent intangible transfers of knowledge and know-how.[56]

Pending the strengthening of international instruments, EU member states are encouraged to make special efforts to raise the awareness of financial institutions in order not only to prevent proliferation activities from being financed but also to (*a*) protect European banks from proliferators' malicious intentions; (*b*) improve cooperation between governmental and financial supervisory authorities; and (*c*) encourage the flow of relevant information to financial institutions for exercising financial vigilance.[57] Moreover, the WMD Strategy calls on the European Commission to analyse possible options for promoting the vigilance of financial institutions in the context of combating proliferation financing. As a result, the European Commission took part in the specific Project Team on Proliferation Financing of the FATF Working Group on Terrorist Financing and Money Laundering from October 2008 to February 2010.[58]

Regarding UN Security Council Resolutions 1718 and 1737, the EU proceeded in 2007 to transpose these international measures into law by adopting the so-called Iran and North Korea regulations mentioned in section II. Both regulations contain

[49] FATF (note 43), Paragraph 7(f), Paragraph 8(a), (b), (d), (e).

[50] FATF (note 43), Paragraph 8(c).

[51] FATF (note 43), Paragraph 10.

[52] Ganguli (note 23), p. 623.

[53] FATF (note 47), p. 47.

[54] Council of the European Union, 'Fight against the proliferation of weapons of mass destruction: EU strategy against proliferation of weapons of mass destruction', 15708/03, 10 Dec. 2003, <http://register.consilium.europa.eu/pdf/en/03/st15/st15708.en03.pdf>.

[55] Council of the European Union, 'Council conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems', 17172/08, 17 Dec. 2008, <http://trade.ec.europa.eu/doclib/html/141740.htm>.

[56] Council of the European Union (note 55), p. 5.

[57] Council of the European Union (note 55), p. 16.

[58] See also Bartels, B. et al., *European Banking and Financial Services Law*, 4th edn (Larcier: Brussels, 2010), p. 303.

specific and extensive anti-proliferation measures as well as standard financial sanctions provisions (e.g. asset freeze, non-availability of funds, exemptions and so on), which are very similar to those used in the anti-terrorism and Al-Qaeda regulations. This section focuses on the Iran Regulation due to its complexity as well as its broad political, financial and regulatory implications and repercussions.

The 2007 Iran Regulation has been replaced twice by subsequent regulations, following international political developments and UN Security Council resolutions. The APF-related aspects of the EU's currently effective Iran Regulation no. 267/2012 are as follows.

1. Extensive restrictions on the export and import of proliferation-related goods and technologies pursuant to Article 2 and Annexes I–V.
2. Restrictions on transfers of funds and on financial services in Article 30.
3. The so-called vigilance obligation pursuant to Recital 17 and Article 32.
4. The listing of a number of internationally active banks headquartered in Iran in Annexes VIII and IX.[59]

Of the above provisions, the vigilance obligation of Article 32, which is based on Paragraph 10 of UN Security Council Resolution 1803 (and Paragraph 21 of the later Resolution 1929) concerning Iran, is one of the most challenging issues.[60] The objective of this provision is to require financial institutions operating in the EU to exercise vigilance when monitoring the activities of financial institutions domiciled in Iran or controlled by persons or entities domiciled in Iran that may contribute to the proliferation of sensitive nuclear technology or to the development of nuclear weapon delivery systems in Iran. To that end, Article 32, Paragraph 1 of the Iran Regulation requires financial institutions operating in the EU to (*a*) exercise continuous vigilance over account activity, particularly through their CDD programmes and under their obligations relating to money laundering and the financing of terrorism; (*b*) ensure that in payment instructions all information fields which relate to the originator and beneficiary of the transaction in question are completed, and to refuse a transaction if that information is not supplied; (*c*) maintain all records of transactions for a period of five years and make them available to national authorities on request; and (*d*) promptly report their suspicions to the FIU (or to another competent authority designated by the EU member state concerned) if they suspect or have reasonable grounds to suspect that funds are related to proliferation financing.

The requirement of exercising 'continuous' vigilance presently only targets Iranian financial institutions, and therefore has a narrow scope.[61] Nevertheless, in the opinion of practitioners from the European banking industry, the provision is especially challenging and problematic as it does not specifically define the term 'vigilance', but requires financial institutions operating within the EU to implicitly apply enhanced CDD as the baseline AML/CFT operational standard when dealing with Iranian financial institutions as business partners, a fact that is endorsed by the FATF statements on Iran.[62]

Moreover, it is significant that thus far the AML/CFT regime (including the Wire Transfer Regulation) and the financial sanctions regime of the EU have coexisted side by side, with the AML/CFT regime providing the requisite research tools and the CDD and KYC-based screening procedures for financial institutions in the EU to potentially detect and identify natural and legal persons in their customer base that are listed by the financial sanctions regime. The vigilance requirement, however, inserts a separate set of AML/CFT measures into the financial sanctions regime. In conjunction with the high political and legal profile that characterizes financial sanctions provisions as well as the compliance requirements and enforcement of them, the AML/CFT measures inserted into the vigilance obligation of the sanctions regime against Iran ultimately do not leave any discretion or flexibility for financial institutions in the EU other than to apply enhanced CDD measures. This problem is further compounded by Article 30 of the Iran Regulation, with its complex notification and authorization procedures, which imposes restrictions on transfers of funds and financial services and

[59] The listing of Iranian banks amounts to a virtual severing of all business links (of EU banks) with banks in Iran responsible for the financial handling of the bulk of the country's foreign trade. Bozorgmehr, N. and Saigol, L., 'Iran finds ways to slip grip of sanctions', *Financial Times*, 15 Aug. 2012.

[60] UN Security Council Resolution 1929, 9 June 2010.

[61] However, the present structure of Paragraph 2, Article 32 of the Iran Regulation suggests that this restriction could be expanded for reasons of political expediency so as to include further targets, i.e. other legal and natural persons with a potential (but seemingly unidentifiable) Iran nexus.

[62] FATF, 'High-risk and non-cooperative jurisdictions' (note 44).

implicitly requires banks to check all payments to and from Iran as well as business relationships with Iranian persons pursuant to Article 1 on the basis of enhanced CDD. Article 30 can thus be construed as an additional element of vigilance that, due to its extensive non-targeted scope, places virtually all bank-based transactions with Iranian persons under a general initial suspicion of proliferation financing and money laundering. Therefore, it is justified to say that the provisions of Articles 30 and 32 have to some extent resulted in a sanctions-based 'gold plating' of AML/CFT standards in the EU.

As a result of the Iran Regulation (and the North Korea Regulation), the EU has added a further layer of complexity to its financial sanctions regime. By including AML/CFT and wire transfer provisions within the scope of the Iran Regulation, it has interlinked these two regimes with financial sanctions and created a hybrid regime.[63] Furthermore, it is a troubling that the rise of such a hybrid APF regime harbours the risk of seriously compromising or, in the worst case, rendering the structural integrity and functioning of both regimes ineffective, as the AML/CFT regime follows a risk-based approach, whereas the financial sanctions regime follows a rule-based logic. This could result in a situation in which none of the policy objectives of the respective regime is adequately achieved.

## IV. ISSUES FOR THE EUROPEAN BANKING SECTOR

### Implementation issues

Since the adoption of the APF-related measures, financial institutions operating in the EU have made efforts to implement the requirements with the instruments at their disposal and thereby ensure compliance. Given the hybrid nature and resulting complexity of the EU's APF-related financial sanctions regime, exemplified by the Iran Regulation, financial institutions are confronted with the task of implementing a patchwork of regimes that are not always properly harmonized and that harbour significant compliance and economic challenges and risks. The standards and legislative measures adopted by different institutions at the macro level by the UN, the FATF, the EU and member states are not always coherent and lack clarity. Therefore, substantial efforts are directed at meso-level implementation, where banking associations and competent authorities of EU member states negotiate on actionable guidelines to bring all these standards and regime provisions within the scope of a clear, pragmatic and coherent implementation framework. This allows banks operating at the micro level to observe and execute the laws in their day-to-day business transactions without much friction.[64] Figure 4 shows the regulatory structure and framework of interlinked AML/CFT/APF regime implementation as perceived by banks operating in Germany.

The implementation of such a complex regulatory framework of interlinked regimes places a range of limitations on financial institutions at the micro level. The measures already taken by banks to implement sanctions are geared to their specific situation and needs, including the nature and scope of business activity, the corporate structure, the technical infrastructure and the specific risk exposure pursuant to the risk assessment of the financial institution. An important starting point is the AML/CFT risk assessment that banks are required to conduct on the basis of regulatory requirements.[65] Although specific risk characteristics and profiles may differ from one financial institution to the other, the risk assessment cycle should include: (*a*) a complete inventory of the existing customer/product/transaction structure of the bank; (*b*) the identification of relevant (including APF-related) risks; (*c*) an evaluation of the risks; (*d*) the formulation of appropriate measures and policies to minimize the risks; and (*e*) a regular review concerning the validity of the measures. Should the review not yield any APF-related issues, due to the complexities of the regime, the result of the exercise is to be documented. Moreover, banks are additionally charged with the task of implementing the provisions of the EU's constantly changing APF regime within their risk assessment and management as well as their compliance framework in a timely and structured manner, as stated in the following.[66]

1. Banks are required to screen a potential customer against official EU sanction lists before entering into

[63] See Ganguli, 'The Third AML Directive', Part III (note 4), pp. 804–806; and Ganguli (note 2), pp. 157, 172–185.

[64] Ganguli (note 2), pp. 107, 289–375.

[65] Article 34 of the 3AMLD and Ganguli (note 2), pp. 399–401.

[66] The procedures and recommendations discussed in the following are of an indicative nature and may vary from bank to bank. See Ganguli (note 23), pp. 623–626.

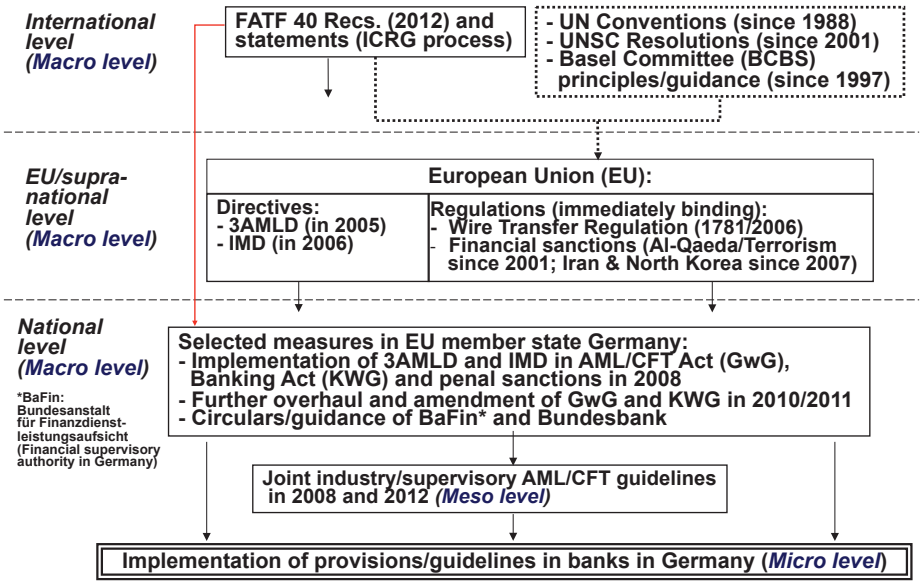


**Figure 4.** Regulatory structure and framework of interlinked AML/CFT/APF regime implementation

*Source*: Adapted from various presentations by Ganguli, I. and Ernoult, J.

a business relationship. In this process, information obtained from other sources regarding a potential customer should be considered when deciding whether a business relationship should be entered into. Irrespective of this, the customer base should be screened with regard to existing customers in case of any amendments to the lists of sanctioned persons pursuant to the Iran Regulation.

2. Information concerning a customer collected either internally or externally within the scope of KYC and CDD measures should also be appraised for the purpose of entering into or maintaining existing business relationships. Moreover, banks should record this information in their documentation and use it to classify the customers into risk categories (e.g. low, medium or high). Each bank should determine the parameters and/or indicators included in the risk cycle on the basis of its individual AML/CFT risk analysis.

3. With respect to documentary credit transactions, in particular, banks should—in addition to screening against official sanction lists (of the persons involved in the business transaction)—check the credit and shipping documents for references to proliferation-relevant countries (e.g. Iran or North Korea) or sanctioned goods and the plausibility of the underlying transaction by applying a risk-based approach. In cases of doubt, the customer should be requested to present an export licence from the export control authorities (the same applies to trade, export and project financing transactions).

4. Additional information and indications regarding the customer or the persons involved in a documentary credit transaction continuously derived in the course of a business relationship should also be used for further KYC and monitoring measures. In this respect, the scope and extent of such KYC measures are always determined on the basis of the risks involved in the individual case.

5. If peculiarities or 'hits' regarding transactions are generated by the research system within the scope of the examination and monitoring measures, the establishment of a graded escalation procedure in the banks is recommended as follows.

a. The bank department responsible for foreign payment transactions should check whether the hits reported in connection with the transaction are obvious 'false positives' (as in 90 per cent of all cases).
b. The remaining questionable transactions should be forwarded to the responsible AML officer in charge, who reviews the facts more closely by considering all legal aspects.
c. If suspicious facts indicating a breach of sanctions law, AML/CFT law or legal provisions countering proliferation financing cannot be established

and the initial doubts prove to be unfounded, the payments should be cleared for further processing.

d. Any suspicions that have been established must be reported to the competent authorities by filing a STR. If possible, the transaction should be intercepted; and the funds should be blocked or frozen, depending on whether the transaction falls within the scope of AML/CFT measures or the sanctions regime. The financial institution should consider terminating the business relationship with the customer and document the process thoroughly for supervisory review purposes.

6. Regarding correspondent banking relationships, a bank may ask the correspondent for written confirmation in which the latter declares its compliance with internationally recognized CDD standards and the entity-based financial prohibitions of the UN. It might be advisable to cross-check the veracity of the information received by consulting publicly accessible, independent and authoritative sources (e. g. to establish whether the correspondent bank has recently faced any public charges, supervisory enforcement actions or sanctions). Whether such measures will ultimately result in any value added in terms of fulfilling the AML/CFT and financial sanctions obligations as well as in terms of compliance risk mitigation and management for the requesting bank is debatable.

However, the CDD, monitoring and internal control measures presented above have their limitations, especially when it comes to monetary transactions and documentary transactions (documentary credit transactions and documentary collection) where the processes are strongly formalized and/or automated due to internationally uniform standards and regulations developed by market practitioners and accelerated processing requirements. This specifically refers to, among other things, the Uniform Customs and Practice for Documentary Credits (UCP) of the International Chamber of Commerce (ICC).[67] Article 5 of the UCP 600 states the following regarding the role assigned to banks with respect to documentary credit transactions: 'Banks deal with documents and not with goods, services or performance to which the documents relate.'

Moreover, the introduction of the FATF and APF-related EU sanctions requirements, with the associated enhanced CDD measures, interferes with existing structures and processes that are internationally standardized in many areas and renders an automated processing impossible. As a result, the affected customers' transactions could become considerably slower, more time-consuming and cost-intensive or even economically impossible. This is especially true for the following areas, which play an important role in international trade.

1. *Documentary credit transactions or letters of credit*. In such transactions, a credit institution agrees in relation to the applicant or customer to pay a certain amount of money to a third party against the presentation of documents specified in advance, whereby the delivery of goods, meaning the export and/or import of goods (the basic transaction), usually forms the economic basis. Since a documentary credit transaction with a proliferation background does not differ in structure from a conventional transaction, a credit institution which has no insight into the overall context has very limited or no means to detect a proliferation background (except if the documentary information furnished is visibly incoherent). This is especially true for goods destined for dual-use purposes.[68]

2. *Documentary collection*. In the case of documentary collection, a credit institution agrees in relation to the ordering party or customer to surrender certain documents to a third party within a certain period of time against the payment of a certain amount of money. This method is frequently used within the scope of international monetary transactions. A content check does not take place, since the task of the credit institutions is limited to a purely formal examination of the submitted documents. Expanding the scope of examining obligations would therefore fundamentally change and challenge the structure and rationale of this method and the related transactions.[69]

3. *Structured trade financing and/or export financing or project financing*. Credit lines or loans, structured trade financing and/or export financing are rather long-term modes of financing a commercial transaction. The underlying objective of the transaction usually

[67] International Chamber of Commerce (ICC), Revision of Uniform Customs and Practice for Documentary Credits (UCP), ICC Publication no. 600 (UCP 600), Paris, 2006, <http://www.iccbooks.com/Product/ProductInfo.aspx?id=456>.

[68] Kümpel, S., *Bank- und Kapitalmarktrecht* [Banking and Capital Markets Law] (Verlag Dr Otto Schmidt: Cologne, 1995), p. 684–708, Paragraph 7.64–7.161.

[69] Kümpel (note 68).

consists of delivering high-quality goods (e.g. a power plant generator) or work performance. Project financing covers, among other things, infrastructural projects or the construction of plants by involving project companies. Regarding the extension of loans, in particular, it might be possible for banks to gain a deeper insight into the background of business transactions and, under certain circumstances, it would be possible to examine more closely whether there is a connection to proliferation purposes. However, it is most likely that financial institutions do not generally have the required technical know-how to make a reliable assessment. In addition, the legal and factual control mechanisms that are required for rapid validation and clarification are lacking in cases of doubt.

4. *Payment transactions*. Concerning payment transactions, a screening of the customer base against official sanctions lists is performed (mostly) in real time in the context of transaction monitoring. Additionally, verification of the intended use as well as an examination regarding the particulars of a transaction is carried out within the scope of the general AML/CFT measures (i.e. account screening) in conjunction with the requirements of the Wire Transfer Regulation. However, due to the high degree of automation required for processing the huge amount of payment transactions, the information supplied in connection with an individual transaction is limited to that absolutely necessary for processing and can, therefore, shed no light on the actual background of the transaction.

## Lessons learned

As previously mentioned, the concepts presented by the FATF are based on imprecise or even unrealistic assumptions and do not provide a suitable basis for clearly distinguishing between high-risk and low-risk customers, transactions and products. This, however, is absolutely necessary in order to understand the difficulties and compliance and economic risks that banks face when implementing and executing the provisions of the complex and hybrid APF regime (see figures 1, 3 and 4).[70] A number of lessons have therefore been learned.

Banks are only involved in the execution of the financial transaction and not in the objectives of the underlying business transaction that may contain proliferation risks. Therefore, they can obtain only limited information, if any at all, about the delivery channels and end users connected with the exported goods. With respect to delivery channels, the requirement to identify possible diversions of sanctioned goods to Iran is clearly not practicable due to the countless actors involved in the export business and the dimensions of global trade.[71]

Moreover, a majority of the underlying business transactions and most of the associated financial transactions do not show any peculiarities or special characteristics when considered singularly (e.g. the export of metal sheets). The transactions, therefore, appear unsuspicious to banks, especially if export control authorities have issued the required export licences. Since an export transaction with a potential (but not clearly recognizable) proliferation background has the same characteristics as a conventional export transaction and the beneficiaries or end users of the payments are not customers of the export financing bank, there is—in contrast to money laundering cases—a lack of conspicuous patterns (typologies) that could serve as a suitable basis for devising red flag indicators.

In addition, procurements for proliferation purposes are channelled by proliferation agents through complex and opaque international networks involving interposed undertakings and fronts acting for intermediate companies and ultimate beneficial owners that are beyond the grasp and control of financial institutions (see figure 2).[72] In this process, the goods and supplies are divided into several individual packages that are unsuspicious when viewed singularly, so that banks are not easily able to identify the proliferation background of the entire transaction.

When a bank does become aware of a transaction with a proliferation-related background, this inevitably happens on the basis of hard actionable information disclosed by parties involved in the underlying business transaction; certifications or declarations issued by export control authorities; or information provided by government intelligence services. Therefore, examination or verification of the proliferation background of a financial transaction on the basis

[70] Ganguli (note 2) pp. 406–414.

[71] FATF (note 43), Paragraph 8.

[72] German Federal Office for the Protection of the Constitution (note 37) pp. 9–12.

of other independent and neutral sources is neither conceivable nor feasible.

Further, banks do not have the policing or investigative powers or analytical capacities available to intelligence services or export control authorities. These competent authorities have the ability to scrutinize the legitimacy of merchandise exports. This problem has been recognized in the FATF 40's INR 7 and Additional Guidance (Chapter 3, Number 8) and addressed by a corresponding recommendation to the authorities to provide additional proliferation-relevant information to banks. Nevertheless, the impression remains that the Additional Guidance imposes the main burden of procuring and analysing information on credit institutions. This is certainly not feasible from the perspective of the banking industry and therefore not a very realistic and productive line of action.

Finally, political decision makers, legislators and regulators should be aware of the following. To the extent to which the banking industry (which is only indirectly involved) should be included in APF measures, past experience shows that only concrete, updated, actionable and detailed entity-based information from authorities concerning (*a*) suspicious proliferation financing activities; (*b*) patterns of business transactions of banks' customers; and (*c*) proliferators has proven to be an effective approach. Therefore, checking the actionable information provided by law enforcement and government intelligence agencies on individuals or companies involved in proliferation by accessing an electronic database via a protected website—along the lines of the European Commission's consolidated electronic list of financial sanctions—might be a viable option. However, it is more likely that EU and UN member states will not be willing to share their hard intelligence with banks, as this could compromise their secrecy as well as national security interests and give rise to data protection issues.

## V. CONCLUSIONS

Compared with the AML/CFT and financial sanctions regimes, the issue of combating proliferation financing is still in a nascent stage. This paper has attempted to trace recent developments and demonstrate that the EU's APF-related measures against Iran and North Korea do not, strictly speaking, constitute a coherent and structured regime, but borrow elements from the conventional financial sanctions regime and the AML/CFT regime in terms of regulatory structure, the use of legal and procedural instruments, and research tools. The APF regime, created as a third pillar in the overall framework of international law and measures to maintain or restore global peace, security and governance, thus resembles a patchwork of provisions (see figures 1, 3 and 4) and can be characterized as a hybrid regime with rule- and risk-based features.

However, since the adoption of the APF-related financial sanctions regulations against Iran and North Korea, banks in the EU have made considerable progress in implementing the requirements of the regime with the instruments at their disposal and thereby creating a robust compliance and risk management framework. A further tightening of the EU's interlinked AML/CFT/APF regime is to be expected after the release of the revised FATF 40 in 2012 and the review of the 3AMLD scheduled for 2013. Additionally, the FATF's continuous 'blacklisting' of Iran as a jurisdiction with a highly deficient AML/CFT framework has prompted supervisory authorities in the EU to require supervised financial institutions to apply enhanced CDD standards to customers with an Iran nexus. Moreover, the EU has adopted further restrictive provisions in its new Iran Regulation (267/2012) regarding customer-, product- and transaction-related due diligence that necessitate the introduction of constant, extensive and complex changes in the existing financial sanctions and AML/CFT compliance systems of banks.

Although the financial sector fully supports these efforts, the resulting regulatory changes are costly to implement and affect all transaction processes, documents and regulations relevant to international trade that have been developed by practitioners over time. There is also the risk that the measures might eventually prove unsuccessful, since the structural issues and deficiencies of the EU's APF-related financial sanctions regime cannot be overcome by constantly adopting new, extensive and complex obligations that are politically motivated and less geared towards the requirements of successful implementation. The scope of the measures is already severely affecting international monetary transactions, documentary credit transactions, the international trade and export financing activities of banks and ultimately the entire international trading system.[73]

[73] Bozorgmehr and Saigol (note 59).

Against this backdrop, in the case of the Iran sanctions, financial institutions in the EU are more or less compelled to regard any customer or business partner (natural or legal person) with a potential (but seemingly unidentifiable) Iran nexus as a potential money launderer and/or person involved in Iran's nuclear proliferation programme. Therefore, they have resorted to subjecting all Iranian customers to the highest possible degree of enhanced CDD. As Iranian nuclear proliferators and their associates (including other witting or unwitting parties) as well as Iranian money launderers are not easily discernible within the framework of CDD and AML/CFT research measures, financial institutions operating in the EU may have to actually consider designating—in contradiction to the targeted approach of the UN and the EU's financial sanctions regimes and the risk-based approach of the 3AMLD—all natural and legal persons or customers domiciled in Iran, with Iranian citizenship or with a potential (but seemingly unidentifiable) Iran nexus as high-risk customers in order to avoid inviting further intrusive review from the competent supervisory authorities and risking hefty fines. What can be observed as a trend in recent years is that financial institutions in the EU are actually severing links with mostly legitimate Iranian business partners and wrapping up their Iran operations altogether—also partly as a response to political pressures from the US Government.[74]

Furthermore, implementation of the tightened requirements of the Iran Regulation has resulted in more or less comprehensive sanctions against Iran due to the interruption of trade and financial transaction links with the country. Such a result appears to be inconsistent with the existing smart sanctions as well as the economic statecraft strategy and policies of the UN. In fact, the measures are not hitting the targeted persons or companies in charge of Iran's nuclear programme. According to observers, they are adversely affecting the majority of the civilian population on an increasing scale, who are facing high inflation and the prospect of economic decline.[75] Past research shows that overly harsh sanctions can have counter-effective consequences, such as increasing popular support for the policy of targeted governments.[76] In the case of Iran, it has been observed that the further tightening of APF-related sanctions has led parts of the Iranian population to 'rally around the flag' and support the present government's nuclear policies, which is exactly what the international community wants to change through the use of these measures.[77]

In view of this, successful implementation of APF-related sanctions needs to be supported by a further intensification of national export control measures. Such measures affect and discipline exporters and could be a suitable basis, and an effective starting point, for a targeted approach to containing WMD proliferation that is consistent with the tenets of the financial sanctions regime of the EU and the UN. In fact, the relevant industries (e.g. in the chemicals, machinery and biological and life science sectors) are already drawing their conclusions from the banking sector's RBA experience by devising their own industry-specific risk assessments that help them to flag suspicious export activities and by setting up specific compliance departments.[78] They should also have proper governmental contact points that can provide them with updated and actionable information. If the banking industry, which is only indirectly involved in the transactions, is to be included in the strategy, past experience shows that the most effective means is providing concrete, updated and actionable information from authorities concerning suspicious proliferation financing activities or patterns of banks' customers. Such indications would enable banks to apply the available compliance instruments as efficiently as possible. This is currently not the case and in practice results in serious compliance problems and risks. However, it is questionable whether governments and their intelligence services would be willing to share such information due to the imperatives of secrecy and national security, which pose serious limitations for governments and economic operators alike. Therefore, from a banking perspective, it would be reasonable to demand that the UN, the FATF, the EU and the competent authorities of the EU member

[74] 'Rückzug aus dem Irangeschäft' [Retreat from Iran trade], *Handelsblatt*, 2 Feb. 2006; 'USA drängen deutsche Firmen aus dem Iran' [USA forcing German companies out of Iran], *Handelsblatt*, 11 Jan. 2007; Bozorgmehr and Saigol (note 59); Faucon, B. and Coker, M., 'Willing banks find profits in legal trade with Iran', *Wall Street Journal*, 4 Aug. 2012; and 'Iran-Geschäfte der Großbanken am Pranger' [Dealings with Iran by big banks criticized], *Börsenzeitung*, 21 Aug. 2012.

[75] Bozorgmehr and Saigol (note 59).

[76] Verdier, D. and Woo, B., 'Why rewards are better than sanctions', *Economics & Politics*, vol. 23, issue 2 (July 2011), p. 220.

[77] Regnault, S., 'Les sanctions contre l'Iran sont inefficaces' [The sanctions against Iran are inefficient], *Le Monde*, 27 Nov. 2012.

[78] See Wiertz, R., Head of Global Trade Control at Oerlikon, 'Implementation of Internal Control Programs (ICP)', Presentation, 25 Jan. 2011, <http://www.osce.org/fsc/75198>.

states—in addition to their focus on credit and financial institutions—direct their efforts at exporters and introduce the necessary changes suggested above in order to facilitate a more integrated, and hopefully successful, implementation of the provisions of the APF regime.

## ABBREVIATIONS

| | |
|---|---|
| AML | Anti-money laundering |
| APF | Anti-proliferation financing |
| BO | Beneficial owner |
| CDD | Customer due diligence |
| CFT | Combating the financing of terrorism |
| EDP | Electronic data processing |
| FATF | Financial Action Task Force on Money Laundering |
| HSBC | Hong Kong and Shanghai Banking Corporation |
| ICC | International Chamber of Commerce |
| KYC | Know Your Customer |
| NPT | Non-Proliferation Treaty |
| RBA | Risk-based approach |
| STR | Suspicious Transaction Report |
| WMD | Weapon(s) of mass destruction |
| 3AMLD | Third Anti-Money Laundering Directive |

# EU Non-Proliferation Consortium

*The European network of independent non-proliferation think tanks*

## A EUROPEAN NETWORK

In July 2010 the Council of the European Union decided to create a network bringing together foreign policy institutions and research centres from across the EU to encourage political and security-related dialogue and the long-term discussion of measures to combat the proliferation of weapons of mass destruction (WMD) and their delivery systems.

## STRUCTURE

The EU Non-Proliferation Consortium is managed jointly by four institutes entrusted with the project, in close cooperation with the representative of the High Representative of the Union for Foreign Affairs and Security Policy. The four institutes are the Fondation pour la recherche stratégique (FRS) in Paris, the Peace Research Institute in Frankfurt (PRIF), the International Institute for Strategic Studies (IISS) in London, and Stockholm International Peace Research Institute (SIPRI). The Consortium began its work in January 2011 and forms the core of a wider network of European non-proliferation think tanks and research centres which will be closely associated with the activities of the Consortium.

## MISSION

The main aim of the network of independent non-proliferation think tanks is to encourage discussion of measures to combat the proliferation of weapons of mass destruction and their delivery systems within civil society, particularly among experts, researchers and academics. The scope of activities shall also cover issues related to conventional weapons. The fruits of the network discussions can be submitted in the form of reports and recommendations to the responsible officials within the European Union.

It is expected that this network will support EU action to counter proliferation. To that end, the network can also establish cooperation with specialized institutions and research centres in third countries, in particular in those with which the EU is conducting specific non-proliferation dialogues.

http://www.nonproliferation.eu

FONDATION pour la RECHERCHE STRATÉGIQUE

## FOUNDATION FOR STRATEGIC RESEARCH

FRS is an independent research centre and the leading French think tank on defence and security issues. Its team of experts in a variety of fields contributes to the strategic debate in France and abroad, and provides unique expertise across the board of defence and security studies.
http://www.frstrategie.org

PRIF Peace Research Institute Frankfurt — HSFK Hessische Stiftung Friedens- und Konfliktforschung

## PEACE RESEARCH INSTITUTE IN FRANKFURT

PRIF is the largest as well as the oldest peace research institute in Germany. PRIF's work is directed towards carrying out research on peace and conflict, with a special emphasis on issues of arms control, non-proliferation and disarmament.
http://www.hsfk.de

IISS

## INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

IISS is an independent centre for research, information and debate on the problems of conflict, however caused, that have, or potentially have, an important military content. It aims to provide the best possible analysis on strategic trends and to facilitate contacts.
http://www.iiss.org/

sipri

## STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.
http://www.sipri.org/