Money Laundering & Terrorism Financing

Key Aspects

Katia Haliskou Supreme Court Lawyer LL.M Criminal Law

INTRODUCTION

Money laundering and terrorist financing represent serious global threats to economic life and society as they further support criminal activity and put in danger the foundations of the rule of law. Money laundering is the process of disguising the illegal origin of a profit. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the illegal activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention. Money launderers are continuously looking for new ways for laundering illegal funds. Economies with developing financial centres, but inadequate controls, are particularly vulnerable, because developed countries implement strong anti-money laundering regimes.

I) DEFINING MONEY LAUNDERING & TERRORISM FINANCING

MONITORING MONEY LAUNDERING

Money laundering involves three stages: the placement stage, the layering stage and the integration stage. The placement stage is the stage at which funds from illegal activity are first introduced into the financial system through diverse ways like change of currency, change of denomination, transportation of cash. The layering stage involves further distancing the illicit funds from their illegal source through transactions like withdrawals in cash, cash deposits in multiple bank accounts, split and merge of various bank accounts. The integration and final phase results in the illicit funds being considered "laundered" and integrated into the financial system so that the criminal may expend "clean" funds.[1]

TERRORISM FINANCING

Terrorist financing means the provision of funds with the intention that they should be used in order to carry out terrorism activity. Given that both Money Laundering and Financing of Terrorism are typically committed through the abuse of financial institutions, the fight against them demands the adoption of a consolidated strategy. Several international bodies like the Financial Action Task Force on Money Laundering (FATF), the United Nations, the International Monetary Fund (IMF), the World Bank, have developed a number of strategies against this illicit activity. Financial Institutions have been called to take appropriate measures. Such measures also include compliance with the financial sanctions set by the United Nations Security Council Resolutions and other actors.

[1] OECD "Money Laundering Awareness Handbook for Tax Examiners And Tax Auditors, Organization For Economic Co-Operation and Development".2009 Available at www.oecd.org/dataoecd/61/17/43841099.pdf

FATF - The Recommendations

The above described illegal activity hinders economic development, because: a) it causes mistrust among communities and thus hinders economic development, b) it diverts foreign investments to more stable economies but for the most part in a way that undermines laws and c) it creates disrespect for values and generates perceptions of unfairness. Domestic and international laws (criminal and civil), regulations and standards have been developed to control money laundering and terrorist financing. Most significant among these are the Recommendations of the Financial Action Task Force ("FATF"), an international inter-governmental body established in 1989 at the G7 summit in Paris which sets the global standards[2]. The obligation in the 40 Recommendations is to report suspicious activity. Suspicious Activity Reports (SAR)s are one of the primary means of sharing information to produce intelligence. The Recommendations are not international laws, but are a set of internationally endorsed global standards. From the perspective of the authorities, the 40 Recommendations provide the main international AML standards[18] and have been endorsed by more than 180 countries. The Recommendations, embodies measures, such as "customer due diligence" ("CDD"). This is a different AML approach to the "hard law" approach embodied in both past international conventions and criminalization of money laundering activities. FATF proposes implementation of legal, regulatory measures for combating money laundering and, terrorist financing. The original Recommendations were drawn up in 1990, reviewed in 1996 and were supplemented with the Eight Special Recommendations on Terrorist Financing in 2001. Together the Forty Recommendations and Special Recommendations on Terrorism Financing set the international standard for anti-money laundering measures and combating the financing of terrorism. In 2000 FATF issued also a list of "Non-Cooperative Countries or Territories" (NCCTs), commonly called the FATF Blacklist. The EU also issued the Fourth Anti-Money Laundering Directive (4MLD) and the Funds Transfer Regulation 2017, which reflect the latest (2012) FATF Standards.

II) PRIVATE ACTORS

Measures combatting money laundering and terrorist financing overlap to a large extent in many professional fields and have influenced the status quo of financial life. All sectors involved in the intermediated chain in a direct or indirect way are committed to respect international standards with regard to money laundering and the financing of terrorism. Business actors have knowledge about clients that is not available to the regulator and are expected to make risk assessments of their customers. Private sector is expected to survey and manage risks of this illicit activity. These regulations instruct private businesses to report transactions that they consider suspicious giving them criteria as to what transaction to report. Based on their own knowledge of clients, business actors are to decide what firms or persons, and which transactions, are risky. Banks and other private actors are to make their knowledge and resources work for AML. When referring to private actors, banks are the main partner in this international attempt, but also enterprises and individual professionals. Banks are most at risk of being misused in connection with money laundering

[2] www.fatf-gafi.org/recommendations

and terrorist financing. They have to evaluate what types of transactions are to be categorized as high or low risk. Generally that means monitoring of the business relationship including scrutiny of transactions undertaken compatible to the customer, ensuring that the documents, data or information kept are up to date.

Focusing on: The Banking Sector

Criminals seeking to hide the proceeds of crime among the huge volumes of legitimate business and financial services. As a result, the banking sector overall is to be at high risk of money laundering and at medium risk of terrorist financing. In this framework banks established policies, procedures and systems of internal control to reduce any danger in its dealings with external parties. They also co-operate with other organizations to prevent organized FCMLTF. Wherever possible, they exchange information with peer Institutions, the relevant competent authorities of the States, and with competent international organizations.

Managing the Risks

The effective FCMLTF prevention strategy for a Bank includes the following:

1) Identify the areas (departments) within the business that are most vulnerable to the risks of FCMLTF
2) Monitor the controls on an on-going basis
3) Take account of the changing circumstances
4) Ensure that the strategy and procedures are supported by appropriate resources and database. The latter plays a huge role as it facilitates the circulation of the information. New technologies are a crucial factor in AML. Robust information technology systems have always been critical parts of AML compliance. Lapses in data integrity and surveillance systems are the ones that make firms vulnerable.

Know-Your-Customer (KYC) Standards

Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a Bank to measure its risk. This is particularly relevant in the context of related counterparties and connected lending. More specifically: The Know Your Client form is a standard in the investment industry that ensures investment advisors know detailed information about their clients and their financial position. Know your customer processes are also employed by companies for ensuring their proposed agents, consultants, or distributors are anti-bribery compliant. Banks and export creditors are demanding that customers provide detailed anti-corruption due diligence information. KYC procedures for Banking operations include routines for the management oversight, systems and controls (e.g. Customer Due Diligence -CDD-) in consistency with FATF guidance[3] . Before examining a transaction, a Bank should be satisfied that it has gathered information sufficient to give a view as to the identity of the ultimate (beneficial) owner

[3] Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing, High level principles and procedures, June 2007

and how ownership is held. For this reason, Banks have adopted the related recommendations of the FATF, which all countries are encouraged to adopt. Usually the CDD measures taken are the follows:

1) Identifying the customer, verifying his identity by a reliable source document, data or information;
2) Identifying the potential beneficial owner
3) Obtaining information on the purpose of the business relationship;

All information should be maintained on record, unconditionally, no less than the minimum period recommended by the FATF (5 years). All necessary records on transactions enable the Banks to comply with information requests from the competent authorities of States. The Banks should exert every effort to detect unusual transactions, understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

The inadequacy or absence of Know Your Customer (KYC) standards can subject a Bank to serious customer and counterparty risks, reputational, operational and legal risks. Reputational risk poses a major threat, since the nature of the Bank's business requires maintaining the confidence of the shareholders, rating agencies, creditors and the general marketplace. Operational risk relates to weaknesses in the implementation of banks' programmes, ineffective control procedures and failure to practise due diligence. Legal risk is the possibility that adverse judgments or contracts that turn out to be unenforceable can affect the operations or condition of the Bank.

Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly[4] because of the lack of an international network. Large international banks typically act as correspondents for thousands of other banks around the world. Because of the structure of this activity and the limited available information regarding the nature or purposes of the underlying transactions, correspondent banks may be exposed to specific money-laundering and financing of terrorism risks (ML/FT risks). When a Bank provides correspondent banking services to responded banks, the Bank should gather sufficient information about a respondent bank to understand fully the nature of its business and correctly assess ML/FT risks on an on-going basis.

[4] Basle Committee on Banking Supervision – Sound management of risks related to money laundering and financing of terrorism, January 2014

LEGAL PROFESSIONS IN THE EYE OF FATF

A revision of the recommendations in 2003 expanded the reach of the Recommendations to bodies that provide "access points" to financial systems, also referred to as "gatekeepers", including legal professionals. The term used for "gatekeepers" is "Designated Non-Financial Businesses and Professions" ("DNFBP"). This extension to control DNFBPs was motivated by FATF's perception that "gatekeepers" were unwittingly assisting organized crime groups to launder their funds by providing them with advice, or acting as their financial intermediaries[5]

Importantly for lawyers and notaries because the CDD and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to them also when they prepare for or carry out transactions for their client concerning managing of assets, creation of companies etc. Lawyers who suspect that their clients are involved with the proceeds of criminal or terrorist activity should make an STR with the relevant FIU and should consider making a report unless filing such a report would violate the rules of lawyer-client privilege, confidentiality and ethics and they are subject to professional secrecy or legal professional privilege.

Money Laundering Red Flags

The ways of money laundering and terrorist financing are rarely similar, so the red flags that appear useful one-day need to be up-dated the next. A United Nations Office on Drugs and Crime (UNODC) 2011 report estimated that in 2009, criminal proceeds amounted to 3.6% of global GDP, with 2.7% (or US$ 1.6 trillion) being laundered[6]. The World Bank produces Worldwide Governance Indicator reports for over 200 countries over 1996-2012[7]. Data from STR (Suspicious Transaction Report) and confiscated assets reports compiled by FATF show that real estate assets formed 30% of all criminal assets in the years 2011-2013[8].

The purchase of real estate is a common method for disposing of criminal proceeds. An appreciating asset and its subsequent sale can provide a legitimate reason for the appearance of funds. Criminals will often seek to create also companies and trusts. Shell companies meaning businesses that do not have any business activities or recognizable assets may be used as serving as transaction vehicles. Another red flag is relating to clients' funds because of their size, source and mode of payment that cannot be justifiable.

Non-Profit organizations and Charities also are huge subject to money laundering. Charities are not subject to the MLRs, but their trustees, employees and volunteers counter terrorism legislation. In the UK for example, charities are also subject to strict civil regulatory regimes by one of three charity regulators - the Charity Commission for England

[5] Shepherd, Kevin L. "Guardians at the Gate: The Gatekeeper Initiative and the Risk-based Approach for Transactional Lawyers." Real Property, Trust & Estate Law Journal 43.4 (2009)

[6] http: llwww.unodc.orglunodclenlpressl releasesl2011lOctoberlunodc-estimates-that-criminals-may-have-laundered-usdoilar-1.6-trillion-in-2009.html

[7] http://info.worldbank.org/governance/wgi/ index.aspx#countryReports)

[8] FATF Typologies Report 2013 available at http://www.fatf-gafi.org/topics/ methodsandtrends/documents/mltf-vulnerabilities-legal-professionals.html Supra n 33

and Wales (CCEW), the Charity Commission for Northern Ireland (CCNI) and the Office of the Scottish Charity Regulator (OSCR). The CCEW has a program which focuses on those charities identified as higher risk for terrorist financing purposes, and has issued guidance to charities to advise them of the risks and help them better protect themselves.

Criminals gaining control also of a licensed gambling business and using it as a cover for money laundering. For this reason, for example in Great Britain all gambling operators offering services must be licensed by the Gambling Commission, including operators based overseas offering services to consumers in Great Britain. In 2016, the Gambling Commission amended its licensing conditions and codes of practice for all operators in relation to the prevention of crime associated with gambling, with focus on AML/CTF provisions.

Finally, another red flag should be noted and that is the High Value Dealer (HVD) as defined under the MLRs, ie. when a business is receiving high value cash payments of €10,000 or more either in a single payment or a linked series, in exchange for goods. Many of these businesses have policies against accepting or making high value payments in cash.

RESOLVING THE CASE

The key role in creating a hostile environment for criminal money have adequate safeguards to prevent themselves from being used for financial crime. In this field the partnership between private actors and law enforcement is vital in limiting abuse of the financial system by terrorists and criminals. The law enforcement response to the risks in the financial services sector is characterized by:

1) Development of intelligence and investigation of the criminal entities involved
2) Working with the financial sector to enable information sharing to improve the development of intelligence to target criminal activity
3) Engagement with international partners
4) Working with the regulated sector to improve its assessment of the threat

Not following the Regulations seems a dead end. The New York State Department of Financial Service (NYDFS) and the UK Financial Conduct Authority recently issued penalties of more than $600 million for AML failings at Deutsche Bank from 2011 to 2015 in connection with securities trades originating in Russia[9]. Forex Bank in Sweden had bad publicity and a severe fine in 2008. After a review by the FSA (FI 2008), the bank was charged to pay 50 million SEK (approximately 5 million Euros) for not adhering to regulation.

[9] Sven Stumbauer, Managing Director, Alix Partners Five steps for anti-money- laundering compliance in 2017, Article, https://internationalbanker.com/finance/five-steps-anti-money-laundering-compliance-2017

III) PUBLIC ACTORS

According to FATF Regulations countries should understand the money laundering and terrorist financing risks and take action adopting relevant policies, including designating an authority to coordinate actions to assess risks. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures. Countries should require financial institutions and other businesses and professions to take either action to mitigate their money laundering and terrorist financing risks. They also have to criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention, taking legislative measures, to enable their competent authorities to freeze: (a) property laundered and (b) transfers' procedures. Such actions will permit to identify, property that is subject to confiscation and take measures. As to terrorist financing it is recommanded to criminalize such actions on the basis of the Terrorist Financing Convention. In this framework, a recommandation proposed by FATF is included to impose financial sanctions to comply with United Nations Security Council resolutions. The resolutions require also countries to freeze without delay the funds or assets involved in such activity and review additionally the adequacy of laws related to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused as it is already mentioned above.

IV) DRAWBACKS – CONCLUSION

This policy – partnership, proposed by the regulator unofficially, is not really recognized by the private actors both banking sector and commercial businesses especially by the latter. This implementation unsettles their organization's system and influences negatively the relation between business and customer. But private actors cannot opt out because they risk severe fines or even criminal charges. To mention also that following this policy, was an expensive undertaking because of the new computerized systems and trained personnel. Additionally, in the operational level it is too difficult to distinguish between suspicious and simply unusual transactions. Normal, unusual and suspicious have different dimensions in every country because of cultural differences, for instance cash payment is an unusual form in Norway but very common in Greece. Another issue is the restrictions imposed by bank's policies not to share sensitive information which reduces their reputation. From one moment to another, big financial institutions became big brothers. Banks lost their liability by offering easy information (given by clients) to the authorities for taxation purposes. And what about sharing information for potentially guilty but finally innocent clients. Is there a liability for sharing privileged information for no lawful reason? Isn't there a conflict as to GDPR? And the most significant which remains is that despite of AML-efforts to detect criminal activity, the outcome does not seem to be successful. Banks are taking action but there are hardly any convictions of money crimes and money laundering. Unless success is to collect money by imposing sanctions to the banks for not implementing the Regulations.

Ending up this attempt to approach some of the important points of the above regulations, it should be said that it is recognizable that these reforms aim to improve the law enforcement response to criminal financial activity in the name

of corporate transparency. But it is questionable if trying to catch or limit this illegal activity, a greater damage in people's personal lives is taking place, whose liberty, independence and equality are internationally and constitutionally protected as sovereign rights.

REFERENCES

1. Basle Committee on Banking Supervision: Sound management of risks related to money laundering and financing of terrorism, January 2014

2. Bergström, M., Svedberg Helgesson, K. and U. Mörth. 2011. A new role for for-profit actors? The case of anti-money laundering and risk management. Journal of Common Market Studies DOI:10.1111/j.1468-5965.2010.02167.xBexell

3. Council Framework Decision: European arrest warrant and the surrender procedure between member states 2002/475/JHA – 13 June 2002

4. Directive 2015/849 of the European parliament and of the council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing – 20 May 2015

5. FATF, The FATF Recommendations, February 2012

6. FATF, Combating Proliferation Financing: A Status Report on Policy Development and Consultation (Status Report), February 2010

7. FATF, Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing, High level principles and procedures, June 2007

8. General Assembly of the United Nations, International Convention for the Suppression of the Financing of Terrorism (1999)

9. International Standard on Auditing

10. OECD, Bribery Awareness Handbook for Tax Examiners, 2009

11. Paolo Mauro, 1997, IMF Economic Issues, Why Worry About Corruption?

12. Security Council Resolutions, 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), and 1929 (2010)

13. Shepherd, Kevin L. "Guardians at the Gate: The Gatekeeper Initiative and the Risk – based Approach for Transactional Lawyers" Real Property, Trust & Estate Law Journal 43.4 (2009)

14. Sources of information

- Transparency International's Corruption Perception Index
- (http//www.transparency.org/research/cpi/overview)

- ABA website (http:llwww.americanbar.org);
- CCBE website (http:llwww.ccbe.edu);
- IBA website (http:llwww.anti-moneylaundering.orgl)

15. Stumbauer Sven "Five steps for anti – money – laundering compliance in 2017" Article, https://internationalbanker.com/finance/five-steps-anti-money-laundering-compliance-2017

16. United Nations-Office of Drugs and Crime and IMF, Model Legislation On Money Laundering and Financing of Terrorism (2005)

17. Uniform Framework for Preventing and Combating Fraud and Corruption, September 2006

18. The World Bank, Procurement Guidelines and the Guidelines for Selection and Employment of Consultants