ИКОНОМИКА И УПРАВЛЕНИЕ, ГОД. I, №3

проф. д-р ДЕЗМЪНД МАКФОРЪН
ЮГОЗАПАДЕН УНИВЕРСИТЕТ "НЕОФИТ РИЛСКИ", гр. БЛАГОЕВГРАД

ANTI-MONEY LAUNDERING REGULATIONS: PROBLEMS AND PERSPECTIVES

Prof. Dr. DESMOND McFORAN
SOUTH-WESTERN UNIVERSITY "NEOFIT RILSKI", BLAGOEVGRAD

Abstract: This paper looks at the broad spectrum of the global problem of money-laundering and how international reaction to this phenomenon has resulted in strict regulations with which all banks must comply, by creating internal systems and procedures for compliance with anti-money laundering regulations. The fact that these regulations have been significantly widened to include accountants and lawyers, for example, makes us all – to a greater or to a lesser extent – subject to these regulations. How the European Union and the United States have responded is also discussed, as is the relationship between these regulations and Basel II.
Key words: AML, enterprise, securities markets, correspondent bank, customer, shell banks, compliance.

Money-laundering is not a new phenomenon. All criminals have always sought to mask the link between the crime and the money which it generates, so that they could enjoy the benefits of their criminal activity. If, however, the criminal perceives no threat to his money, then there is no need to launder it! However, it is estimated that money-laundering accounts for the staggering amount of between 2-5% of global GDP.

1. A BRIEF HISTORY

Until the 1980s, law enforcement was not particularly active in either finding or recovering the financial proceeds of crime. However, with the exponential growth of the narcotics trade during the 1980s, the 'crime bosses' of the trade began to be individually targeted and, the investigations which ensued, were concentrated on following the 'money trail' coupled with the laundering process. It then became clear, that the most effective way of stopping the money flows was to make the laundering process itself, a criminal offence.

In 1988, the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention), initiated a major paradigm-shift in the way in which the major industrialized economies viewed money-laundering. In 1989, the G7 countries decreed that money-laundering posed a major threat to the global financial markets and systems, by distorting markets, providing unfair competition, undermining smaller economies, creating political instability and by encouraging and supporting corruption – both in governments and within financial institutions.

This caused the G7 to create the Financial Action Task Force (FATF), with members who were drawn from officials of the OECD countries, together with some selected others including the European Commission. The FATF was charged with identifying international 'best practice' in combating and preventing money-laundering. The publication of these standards in 1990 is known as the FATF Forty Recommendations.

By 1996, most member countries had enacted legislation to reflect the FATF's 1990 recommendations. In that year, the FATF introduced new and altogether more stringent Anti-Money Laundering (AML) regulations. One of these was to widen the 'predicate offence' term to cover al serious crimes, including proceeds from fraud, tax

evasion, insider trading, investment scams and corruption.

Following 11 September 2001, the FATF released eight new special recommendations, aimed at attacking terrorist financing and, that such offences be designated as 'money-laundering predicate offences'. (1) However, the problem arose as to how legitimately earned money which was subsequently utilized for terrorist activity, could be deemed a 'predicate offence'? The result of the ensuing debate was the creation of new legal obligations to identify suspicious transactions that might be related to terrorism, coupled with extensive powers to block and freeze such transactions.

In 2003, there was a further paradigm-shift when, in that year, the FATF reviewed both its original recommendations and its First Revision. The result was that both the scope and the content changed. The definition of a financial institution was widened to include (not just the original banks, insurance companies and those involved in the securities markets), casinos, gem dealers, real estate agents, bullion dealers, accountants, lawyers and financial advisers. At the same time, all the other provisions were both strengthened and expanded. These provisions cover:

- "Know Your Customer" (KYC);
- the reporting of suspicious transactions;
- the verification of identities;
- the avoidance of shell banks;
- the avoidance of anonymous accounts;
- the institutionalization of AML policies;
- the scrutiny of high-risk customer activity;
- the expert training of staff.

In order to secure compliance with these newly-strengthened and newly-widened obligations, regulators had to enhance their response to non-compliance.

The reason for this, was that criminals are now seen to be vacillating between cash-based money-laundering activities and banks and the financial markets. The derivatives and securities markets are seen to be particularly attractive to money-launderers, because a broker can launder money through a quite legal transaction, with absolutely no need to ever make a false accounting entry!

The aim of the money-launderer, is 'paper-trail avoidance' and, that is why cash-intensive 'front' businesses are favored. These are businesses such as restaurants, bars, tourist hotels, pawnbrokers, travel agencies, construction companies, automobile dealerships and jewellery merchants. Such businesses can use false-invoicing, ghost employees and inflated expenses, in order to create fictitious cash-flows and transactional patterns (both in value and in velocity), so that they ultimately appear to be normal.

2.AML IN THE UNITED STATES (US)

The US Bank Secrecy Act (BSA), requires institutions to both track and report cash transactions in excess of designated thresholds, to have systems in place for the detection of either unusual or suspicious transactions or activity, and to report suspicious activity. In addition to this, the Patriot Act was enacted in October 2001. The current legislation – in line with FATF recommendations – has additionally extended AML to include brokers, dealers and commodities traders as well as non-financial entities, the insurance industry and investment advisors.

There have also been new and additional requirements imposed on financial institutions to verify customer identification. Similarly, the correspondent relations between banks have come under even greater scrutiny, as have private bank clients and foreign shell banks. In order to ensure that such relationships ate not improperly conducted, financial institutions in the US must now obtain certificates from their foreign customers (whether individuals or correspondent banks), which certify that they are not shell banks and, in turn, that they hold no accounts for foreign shell banks.

Additionally, US banks and financial institutions are now required to perform enhanced due diligence on both foreign correspondent banks and foreign private bank clients – in particular, on clients either from off-shore jurisdictions, or, from jurisdictions which are deemed to be 'non-co-operative countries or territories'. Private bank clients are designated as being those who maintain either a relationship with a US financial institution, which is worth more than US$1 million, or who are deemed to be 'politically exposed persons'.

In order to prevent US institutions from dealing with forbidden individuals or jurisdictions listed by the Office of Foreign Assets Controls, the Patriot Act imposed a "Customer Identification Program" (CIP). This requires US financial institutions to collect a minimum amount of identifying information from all customers – individual, institutional or beneficial. Anonymity *per se* is totally forbidden and, indeed, US banks cannot process outgoing funds transfer transactions, unless all parties are named.

However, it is currently estimated that more than 3,200 US banks, 6, 000 brokerage firms and 4,400 insurance companies have yet to even begin to implement basic 'watch' procedures. And yet, between 2003 and 2005, more than US$632 million was spent in the US on AML technology and services. During 2005, however, the rate of banks and other financial institutions taking up measures to comply with AML requirements has risen considerably. This is probably a "knee-jerk" reaction to three specific instances which took place in the US in 2004, where AML regulators issued heavy fines for AML non-compliance. On 10 May 2004, UBS was fined US$100 million for illegally transferring dollars from a Federal Reserve account to Cuba. Five months later, on 12 October, AmSouth Bank of Birmingham, Alabama, was fined US$10 million for AML violations. Six weeks later on 30 November, the Bank of New York was fined US$24 million also for AML violations. These extremely high-profile cases, have put the US financial world on notice that the AML regulators seriously mean business.

3. AML AND THE EUROPEAN UNION (EU)

In June 2004, the European Commission presented a proposal for a Directive on the "Prevention of the USE of Financial Assets for the Purposes of Money-Laundering and Terrorist Financing." (2) The Third Directive is an attempt to ensure a coherent application within all member states (whether inside or outside of the Euro-zone), of the revised FATF Forty Recommendations. (3) On 7 June 2005, The Council of Ministers for Finance and Economic Affairs of the European Union (ECOFIN), approved the Third Directive together with the amendments of the European Parliament of two weeks earlier. This Directive introduces a risk-based approach, whereby banks are obliged to implement customer due diligence requirements proportionally to the concrete risks involved. It is also recognized therein, that risks may differ depending on the interaction of the type of

Customer,
Country,
Transaction.

It is also recognized that, in order to compile information on the identity of customers as well as beneficial owners, banks will need to rely upon the quality of the information provided by the customers themselves. European banks will be able to share this information with other banks and institutions via the principle of "mutual recognition", therefore avoiding the need for customer due diligence for each and every cross-border transaction. This was agreed as an important aspect of the new Single European Payments Area (SEPA), which is due to come into force between 2008 and 2010 within the Euro-zone area of the EU.

The Third Directive also defined "beneficial owners", "politically exposed persons" and "shell banks" in a way which preserved the basis of current European law. A "beneficial owner", is defined as

"… the natural person who ultimately, directly
or indirectly owns or controls 25% or more of
the shares or of the voting rights
of a legal person," (4).

"Politically exposed persons", are now defined as:

"… natural persons who are or have been
entrusted with prominent public functions
and immediate family members or persons
known to be close associates of such persons." (5)

Similarly, the Third Directive now defines a "shell bank" as:

"… a credit institution or an institution
engaged in equivalent activities,
incorporated in a jurisdiction in which
it has no physical presence, involving
meaningful mind and management,
and which is unaffiliated with a regular
financial group." (6)

The importance of these definitions, is that Europeans are showing themselves to be much more pragmatic than their US counterparts. It is now generally accepted within financial circles in Europe for example, that the idea of 'knowing your customer's customer', is generally an unworkable option. Interestingly, the Third Directive also quite specifically prohibits any disclosure whatsoever to customers, that information relating to their transactions has been transmitted to the authorities. (7) However, members of the same financial group are permitted to share such information with each other under certain specific circumstances. (8)

Member countries of the European Union will have to implement the Third Directive in full, within a two-year period following its publication in the Official Journal. Yet, it should be pointed out here, that AML regulators in Europe have been equally as vigorous in the fulfillment of their regulatory obligations, as have their American cousins!

As far back as 2000, the United Kingdom (UK) enacted the Regulation of Investigating Powers Act. Two years later saw the enactment of the Proceeds of Crime Act containing comprehensive AML regulations. These regulations require UK banks to maintain a high level of provision against litigation exposures, which negatively affect a bank's capital adequacy ratios. Important legal cases under this legislation were the fines handed out by the UK Financial Services Authority (FSA), the country's AML regulators, of GBP 2.3 million to Abbey National Bank for failing to comply with AML regulations; the Bank of Scotland and Northern Bank (Northern Ireland) were fined GBP 1.25 million for failures to identify customers and for failing to keep records of customer identification; the Bank of Ireland was fined GBP 375, 000 for failing to detect a series of high-risk cash transactions. (9)

4. AML AND ITS RELATIONSHIP TO BASEL II

The regulations of Basel II, are designed to make banking safer, by determining the minimum capital which banks must reserve, in order to absorb potential losses from market credit and operational risks. By the same token, AML legislation is designed to protect the interests of genuine customers (on the one hand) while also avoiding liability exposure on account of failure to report suspicious transactions to the regulatory authorities, in a timely manner. To do this, however, banks will be required to amass and process a considerable amount of historical data.

Boards of Directors of banks must know and be able to act on the following::

I. major aspects of operational risk as a distinct category of risk;

II. continual internal audit of the bank's operational risk management system;

III. to ensure that "Risk-Mapping' and 'Key Risk Indicators" are used to assess operational risk;

IV. ensure regular monitoring of operational risk profiles and material exposure to losses.

Collating data under AML procedures, is directly related to the data now necessary under Basel II requirements. Before Basel II is implemented, banks will be required to maintain three years of historical data. Basel II is expected to come into force in 2006-7.

Provided that a transactional framework is designed for AML that is also aligned for Basel II requirements, banks will be able to make the best use of their information without having to invest in multiple systems. Basel II addresses both credit risk and operational risk, and these two aspects of banking risk management cannot be tackled successfully with poor data. In any case, poor data is the major barrier to effective risk monitoring and management. Similarly, a failure to implement AML, also adds to operational risk. A failure to meaningfully address operational risk can also result in total catastrophe, as has been shown in recent years - *viz.* the Barings Bank and also the Enron scandals.

5. AML AND THE RESPONSIBILITIES OF ALL FINANCIAL INSTITUTIONS

In order to ensure compliance with AML, all financial institutions must have in place effective policies and procedures to meet these expanded regulations and obligations. This also applies to Bulgarian banks. These policies and procedures can be delineated as follows:

1.An enterprise-wide awareness of all staff of the current AML requirements.

2.There must be thorough training which is directly related to the roles of individual staff members and their operational duties, e.g. account managers, tellers, back-office staff, senior management, compliance officers, together with those who develop new products.

3.Account managers and other staff must be thoroughly versed and completely knowledgeable about each customer, together with the conduct of extensive and expensive due diligence when such is deemed to be necessary.

4.Those entities with which the enterprise does business, must be thoroughly screened by equally rigorous procedures.

5.Effective software must be employed throughout the enterprise, which can assist in identifying unusual transactions.

6.An effective relationship must be developed with the regulatory authorities and with their regulators.

7.Expenditures on software and training must be whole-heartedly supported.

8.There must be an enterprise-wide recognition that there is some business which it is simply not worth having, and that such business is better avoided.

9.There must be a total and unequivocal commitment on the part of the Board of Directors towards AML policy, both domestically and internationally.

Financial institutions, particularly the larger ones, operate globally. Therefore they are subject to financial regulators in every jurisdiction in which they operate. For example, a Singapore bank which has branch offices in London and New York, will have to meet all US, UK *and* EU AML standards, both in the UK and in its domestic operations. Under the US Patriot Act, regulators can require that US banks that have correspondent banking relations with other banks, cease those relationships, if the correspondent bank does not meet US AML standards.

Similarly, compliance failures mean that the perceived image of a bank is one in which the perception will be that the bank has a clientele made up of corrupt politicians, failed businessmen, fraudsters, organised criminals and terrorists!! This is not a rosy prospect for future business! Therefore, AML compliance on the other hand, requires that banks 'Know Your Customer' (KYC), and is able to detect changes in account activities such as changes in funds volume. This invokes the

necessity for high-quality record-keeping, all of which is extremely sound business practice.

Apart from KYC, the key to AML controls is also the constant monitoring of transaction flows. This is important because of the concept of 'layering'. 'Layering' is the technique which involves routing funds through multiple accounts in a chain, in order to hide the origin of the transaction. It is a method widely used by money-launderers.

6. THE CURRENT PROBLEMS OF AML COMPLIANCE

AML detection systems have evolved from being simple rules-based systems into systems which use an anomaly-based approach. Rules-based systems are designed to uncover specific transactions or patterns, which are associated with criminal financial activity. However, the problem with terrorist financing – as has been pointed out above – is that the transaction starts out with 'clean' money, usually occurring in much smaller amounts than those to be found in traditional money-laundering.

The anomaly-based approach pays special attention to unusual transactions and/or activities, which would not be considered 'normal'. This is accomplished by building profiles of past account activity, or, by creating 'peer groups' of accounts which should behave in a similar manner. This information can then be used to provide analysis by producing predictive techniques such as *decision-trees, regression analysis* and *neural networks* to build models which score any new activity as to its likelihood of being suspicious.

The whole area of AML detection, has been made doubly more difficult, because of the evolution of electronic banking and other modes of funds transfer. The scale of the problem is such, that estimates of illicit cash flowing through US banks and brokerage firms in 2003, amounted to more than US$300 billion. In the same year US$11 billion was spent on new technology. In fact, very few institutions have by September 2005, found a way to install a centralised customer-identification system that provides a single customer ID, together with a view across all the relationships of the customer for the institution. For example, many of the largest global banks which have been created through acquisitions, still have divisions which are unable to communicate with each other. Another factor for European banks is the large number of their internet customers. Here, the problem is particularly acute, because currently, there is no system available which can integrate internet banking with mainstream banking procedures.

As a kind of 'stop-gap' measure, some financial institutions have adopted a simple 'payment transaction filter' in order to discover suspicious activity, whereby high-value transactions or priority messages are manually checked for AML compliance. The paradox with this approach is, however, that the penalty for holding up a transaction which later proves to be 'clean', is much higher than the penalty for letting-through transactions that seldom prove to be 'dirty'!!

Other banks have adopted a more integrated approach, whereby the AML compliance 'engine' sits on top of the core banking software, analysing and reporting on all transactions, whether internal or external. The newer generation of AML systems, are also able to 'learn' and to adapt to new patterns and schemes as and when they arise, simply by achieving a contextual understanding of customer behaviour in order to analyse risk. Such newer generation of systems are also able to identify any form of unusual behaviour across all applications for banking products i.e. trade management, loans, credit/debit cards and payments within the banking organisation.

Many of these applications and approaches have, however, been of a piece-meal nature and, they have been targeted towards areas and regions which were deemed to be of absolute and critical necessity. Unfortunately most banks have

made little or no specific efforts to derive benefits from their investments through either better management or of the re-use of data and processes for multiple purposes. To be effective, an AML system requires an enterprise-wide approach, together with a well-constructed compliance programme. This should mean that messages which are post-transactional confirmations – such as bank advice notes and statements – can be left out of the AML compliance procedure. All payments and asset-transfer messages can then be passed through a central AML-compliant filter and a common payment gateway.

However, serious problems still remain to be resolved in the area of AML-compliance and coverage. Once a transaction that proves to be a 'front' for money-laundering is discovered, how it will be dealt with, is still a 'grey' area. An organization with a global operation faces a tough challenge. If the party to the transaction is lucky enough to be living in a 'soft' regulatory regime, the funds will simply be returned back with the reason for doing so being attached. Otherwise, in a 'hard' regulatory regime, the funds will be blocked or frozen by the receiving or sending banks.

7. CONCLUSION

Stringent compliance with AML regulations to the fullest extent, is an enterprise-wide investment in a business model for risk management. As such, it will also, inevitably, lend support to a long-term business transformation. By linking AML into a wider fraud detection strategy, financial institutions will benefit from more effective detection and, therefore, increased fraud loss savings.

Similarly, an AMNL solution will provide an enhanced customer resource management system. Information regarding the source of funds, how the customer utilizes those funds, basic account information and product preferences, is already available in various departments of every bank. The challenge is to aggregate this information into a more behaviorally-oriented context, in order to support broader mandates. These will probably include an analysis of customers' transactional behavior in comparison to 'normalized' activity, risk, the linking of customer relationships, accurate and timely filing and retrieval systems, with both adaptability and expandability.

Finally, all accountants, lawyers and financial advisers, should be aware of their responsibilities to understand the current international regulations and requirements, and the fact that they, too, are subject to them. The same is true of all businesses in the cash-intensive 'risk' sector. Ignorance of the law is no defence, and the year of Bulgaria's accession to the EU is fast approaching. It is quite clear that the US and EU regulators are taking AML seriously. It behooves everyone who is in any way connected to the financial markets and institutions in Bulgaria to take particular note, and to adapt their organizational response accordingly.

REFERENCES

1. FATF: Special Recommendation 2001. Especially SR2.
2. See also Directive 2001/97/EC 10 June 1991; Directive 2001/97/EC 4. December 2001.
3. FATF 40 Recommendations, Enlarged #rd. Revision, June 2003.
4. Article 6.
5. Article 3.10.
6. Article 3.11.
7. See Article 25.
8. *Ibid.*
9. P. Robinson "Anti-Money Laundering Regulations – Next Generation Developments" in *Financial Crime* FSA 2005; also "How Banks are Facing Up to the Challenge" in *Global Anti-Money Laundering Survey* KPMG 2004.