PREVENTION OF MONEY LAUNDERING (AMENDMENT) BILL, 2008: AN ANALYSIS

Manish Jain & Vikas Jain

INTRODUCTORY THEME

There has been much concern about the terror funds coming into country. In addition to that it is also widely believed that the stock market can also be potential investment destination for terrorist groups. In absence of the adequate laws and enforcement mechanism in place, it is difficult to trace the source of money coming into the country and going outside from the country. Given the above context, anti money laundering laws and regulations assumes utmost significance. Prevention of Money Laundering (amendment) Bill , 2008 (PMLA) is yet another mile stone in the vide spectrum of anti-money laundering initiatives by government of India. Minister of state for finance Pawan Kumar Bansal on Friday (18 October, 2008) tabled a bill to amend the Prevention of Money Laundering Act , 2005 (PMLA) in Rajya Sabha. This Bill introduces new category of offences that have cross-border implications for fighting terrorism. Insider trading and market manipulation will be treated as a laundering offence and invite stricter punishment. Offences related to human trafficking, smuggling of migrants, piracy and environmental crimes, over invoicing and under invoicing under customs are also punishable under PMLA. With the passing of Prevention of Money Laundering (Amendment) Act, all casinos, payment gateways like Mastercard, Visa and Western Union and even Credit Card deals will be monitored by law. These organizations will be required to report details of all suspected transactions to the government.

MONEY LAUNDERING ; CONCEPT

Money laundering involves disguising financial assets so that they can be used without detection of the illegal activity that produced them. Through money laundering, the launderer transforms the monetary proceeds derived from criminal activity into funds with an apparently legal source.

In fact, today all financial institutions globally are required to keep an eye on, possibly examine and report, transactions of a suspicious nature to the financial intelligence unit of the central bank in their respective countries. While the US woke up to the necessity of anti-money laundering preparedness (or the lack of it) after September 2001, there are concerns that it might take our very own 9/11 to learn it the ‘hard way’. In India, one of the functions of the Financial Intelligence Unit (FIU) is to review suspicious transactions reported by the banks.

ANTI-MONEY LAUNDERING

The US and the UK reeling under the current credit meltdown recently set up a joint working group to move towards a more robust financial monitoring and regulatory environment. The purpose of this joint group is to explore common or similar rules and guidelines operating in their financial markets. With the US and the UK financial markets having a reach far greater than their physical boundaries, this may be one of the first signs of greater collaborations amongst regulators and impacting global economies.

On the anti-money laundering (AML) front, this does raise readiness issues in the Indian financial sector, which is heading towards fast-paced integration with the global financial systems. An assessment would be required of how updated our AML regulations are and how well is the financial services sector geared up in systems and processes to meet with requirements, which would become the *de facto* global standard with the US Federal Reserve and the British Financial Services Authority (FSA).

PRESENT REGULATORY FRAME WORK

The Prevention of Money laundering Act, 2002 was brought into force in 2005 to prevent money- laundering and to provide for confiscation of property derived from, or involved in , money laundering. At present, the mandatory reporting requirement is applicable on banks, financial institutions and intermediaries. Under the rules, every banking company, financial institution and intermediary has to maintain a record of all transactions for 10 years. Records of all transactions above the stipulated limit submitted to Financial Intelligence Unit (FIU), which manages the data and deciphers it into intelligence, to be used by various agencies. The new entities that are proposed to be brought under the PMLA will now have to report details of transactions to FIU.

Indian banks

Some of the Indian banks have the systems, but they are highly fragmented. They are not integrated and do not allow the access of all customer-related data on a system. This becomes even more relevant from a transaction-monitoring system perspective. The anti-money laundering laws require banks to capture suspicious transactions and report these.

Foreign Banks

All foreign banks providing correspondent banking services to their Indian counterparts are required to provide a certification that the correspondent bank does not do business with shell banks. Declarations regarding this would need to be made by the Indian banks to meet the requirements of the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). The challenge, however, is of identifying the relevant customers across the bank in an efficient manner.

Financial Institutions

Financial institution are required to undertake certain additional measures against a jurisdiction or an entity wherein, it's determined that any of these are high-risk and, thereby, are of 'prime money laundering concern'.

Financial institutions required strengthening their record-keeping procedures to ascertain the identity and address of the participants to a transaction, specifically the beneficial owner of the funds by obtaining information on his/her accounts operating in the country by a foreign person.

THE EFFECT OF THE PREVENTION OF MONEY LAUNDERING (AMENDMENT) ACT , 2002

Once the Act comes into force, payment gateways such as Visa and MasterCard, money changers, money transfer service providers and casinos will soon come under the ambit of India's money laundering law and face mandatory reporting obligations. The bill incorporates provisions to combat financing of terrorism and it introduced a new category of offences which have cross-border implications.

This bill ensures that the investigating agency can attach any property and search a person only after completion of investigating. it has also enhance the period of provisional attachment of property from 90 days to 150 days.

The legislation has also empowered the Enforcement Directorate "to search premises immediately after the offence is committed". This bill also enables the Central Government to return the confiscated property to requesting country in order to implement the provisions of UN Convention Against Corruption. By adding certain offences in part A and Part B of the schedule of Act, it has expended the scope of the Act.

TECHNOLOGY AND MONEY LAUNDERING

Technology is certainly one of the factors that will play an important role in complying with global requirements, whether in customers profiling for a risk-based approach, simple record keeping, transaction monitoring or KYC (know your customer) needs. Establishing systems and processes for collecting and retaining both identification- and transaction-related records in a manner from where the details can easily be retrieved, as and when required, would be important. This would help comply with all global sanctions lists that need to be monitored.

CONCLUSION AND RECOMMENDATIONS

The technology requirement is not limited to identification of suspicious transactions, but also extends to reporting of these suspicious activities to relevant authorities. Processes will have to be built and documented around these systems as filters will be applied at each level of screening (alert monitor, AML officer, compliance, business, Money Laundering Reporting Officer, etc) before these are finally reported to the FIU.

Approach Of Banks

Adoption of a risk-based approach on AML and its application to the existing customer base (consumer and corporates) would need to be demonstrated to the regulator within a given timeframe. This customer database of the bank would need to be run past the AML risk-based model and high-risk customers highlighted and addressed appropriately. This in turn would mean a significant amount of data cleansing, analytics and mining, in addition to training and communication for the banking staff to ensure adherence and awareness of compliance needs, “suspicious matter reporting obligation,” and on not breaching the tipping-off rules.

Challenges for banks

All this is a significant challenge to banks in India. Those in the public sector have the challenge of getting their systems in place to generate the information required for monitoring and reporting, whereas other banks would face regulatory pressure on compliance and not being caught holding a hot potato.

Unanswered questions

These measures will have the direct impact on the market and the clientele . in addition to that, the implementation of these mechanisms will cost hundreds of thousands of rupees in direct expenditures. The changes will not only affect internal processes and information technology, but also the clientele.

In the near future, it will be necessary to react to certain regulatory changes, especially those regarding client identification, client screening and the monitoring of politically active individuals. Legislative compliance will only be achieved through updates in software and methodology, which do not require significant expenditures.