



Money Laundering - Private Banks caught in a mangle

31/10/2005 by: Peter Wilson, ERI Banking Software Ltd

Discretion and confidentiality is the cachet of the private bank. The Swiss are pre-eminent in this respect. In 1934 it was made illegal for banks and their employees to disclose information about their customers, largely to protect Jewish depositors.

But with the world's financial system awash with ill gotten gains – which some estimates put as high as an annual \$1.5 trillion – the criminal beneficiaries are looking for safe havens through which they can filter money.

The secrecy of Swiss banking may have offered a significant competitive advantage, but it is now more of an Achilles heel. However, Swiss bankers have recognised the threat to a sector which represents 16 percent of the country's gross domestic product. In 1989 Switzerland was a founder member of the Financial Action Task Force on Money Laundering (FATF) set up by the G7 countries. Now, according to the IMF, the Swiss anti-money laundering (AML) measures meet the highest international standards.

The international banking industry, meanwhile, has had its reputation for rectitude tarnished by a string of high profile scandals, particularly in the US, where federal legislation has been bolstered as a result. In 1997 money laundering, and abetting it, was made a criminal offence. Compliance required increased transparency, effectively doing away with traditional secrecy.

The law has been applied with due force and rigour in a number of cases, demonstrating that non-compliance not only risks damaging an institution's reputation but also, with the costs of defence actions and potential fines, threatens the bank's continued existence.

If progress has been made, there is still a long way to go. It is estimated that almost half the "dirty money" circulating is transformed into clean money through the global banking system. Unsurprisingly, regulatory authorities are dissatisfied with the banking industry's response.

So banks are being squeezed between two mighty forces – the ingenuity and adaptability of criminals constantly looking for vulnerabilities in the system, and regulators who, armed with even greater powers since 9/11, are able to name and shame institutions

that don't come up to scratch.

Banks are now obliged to implement AML systems. These must be able to store comprehensive customer information sufficient for the bank to be able to perform due diligence on every prospective and existing customer. The systems must also be capable of monitoring transactions for suspicious activity and the bank should have adequate procedures in place to respond to anything unusual that is detected.

Such requirements are expensive. In 2003 financial firms in Europe and the US spent an estimated \$5 billion – with American institutions having to spend almost \$4 billion of this because of the additional obligations of the Patriot Act. Most of this money went on training, technology and reporting systems.

But confusion persists regarding the definition of suspicious activities and there are no hard and fast rules to stop the determined money-launderer. FATF, and latterly the Wolfsberg group of 12 international banks that have Private Banking operations, have made significant advances by reducing the subjectivity of the monitoring process, enabling banks to spot and report criminal activity.

For example certain types of business are classified according to the US Office of the Comptroller of the Currency as “high risk” businesses. Among these are casinos and leather goods stores, car, boat and aircraft dealerships; securities brokers and dealers; and offshore banks in tax and secrecy havens. Car, boat and aircraft dealerships provide launderers with big ticket items that may be purchased with little customer identification and later sold to provide a “legitimate” source of funds.

Client acceptance must now be subject to strict vigilance. Primary responsibility falls on the banker who sponsors the new customer. Proper documentary evidence of individual identity, corporate provenance, and trustees must be examined. Beneficial ownership for accounts must be established which may be difficult if accounts are held in the name of intermediaries.

Additional diligence is required for persons or sources of funds from high risk areas. For example politically exposed people (PEPs) like politicians, government officials and their families and associates are all at risk. The Basel Committee is also concerned about the implementation of adequate KYC standards or Customer Due Diligence because of the associated risks that poor procedures pose for market integrity.

Banks should have a well defined policy for the identification and then follow up of unusual or suspicious activities. These activities may include account transactions that are not consistent with the due diligence file. For example a customer said that he was doing legitimate business in the Czech Republic but is receiving fund transfers from a bank in Byelorussia. Another warning sign might

be an account that has frequent large pass through, or in-out transactions.

The difficulty lies in being able to distinguish between legitimate and non-legitimate activities. The monitoring, screening and searching process must be able to see through the disguises that obscure illicit transactions. A different approach to detection is gaining acceptance, replacing the rather unsophisticated method of monitoring activity on the basis of thresholds.

After all an unusually large transaction is not inherently suspicious – the customer may have just splashed out on a new boat. Where institutions know their client well and understand the pattern of transactions that are normal they should have in place a means of detecting activity that is outside this norm. This means that just as the due diligence for customer acceptance is based on a risk assessment so too will the monitoring process be differentiated according to risk.

The monitoring technology can then be deployed on a configurable basis according to the profile of the customer and the expected activity. It is timely that the information technology tools for facilitating these processes are gaining in sophistication and capability.

Whatever legal form is given to the regulations in the fight against money laundering and fraud, the framework for effective monitoring and screening should be based on three objectives: KYC – know your customers, KYT – know your transactions and KYP – know your processes.

The elements of KYC include measuring customer compliance from for example ID, final beneficiary ownership and political affiliation data at an individual level. Equally compliance for corporate clients will be assessed from information gathered from auditors and companies house. Blacklist data can be integrated into this process from sources such as Factiva which supplies information on PEPs.

The US Office of Foreign Assets Control (OFAC) provides a list of countries and individuals with whom certain financial transactions are prohibited. So for example for counterparties in Iran financing transactions for foodstuffs and carpets is permissible but transactions in oil are not.

KYC thus enables the bank to quantify the compliance risk of a client relationship by defining a Client Compliance Status. This status can then be used to raise alerts and trigger appropriate bank procedures for action. Similarly a Client Operational Profile can be set up and used as the benchmark against which actual activity is monitored and any discrepancy report to the compliance officer.

Once the criteria for risk assessment are established for each account the KYT component is configured to provide real-time

monitoring of account activity and tuned to ignore false positive cases. So for example payments to non-GAFI countries or reactivation of dormant accounts may create exceptions. The KYT monitoring system should be closely linked with another set of processes that are usefully grouped and controlled under KYP.

KYP supports the activities that arise from a transaction exception report on a case by case basis, managed by a well defined set of workflow templates that control the handling of each incident to a satisfactory conclusion.

The dialogue that has been established between the banking industry, which is developing its own initiatives, and the regulatory authorities, is converging onto common ground. How can effective methods and systems be developed? What is clear is that while the banking industry still operates within disjoint regulatory regimes and the criminal gangs can operate cross-border, the objectives of much of the regulations may be stymied.

However, as the international community braces itself for the battle against big crime and terrorist gangs it is only a question of time before more coherence is built into the financial system. As the criminal world of the money launderer becomes more sophisticated, so the technology and processes that are deployed by the banks to meet this challenge will have to become smarter.