Indian Banks' Association

IBS INTELLIGENCE

AML Technology

Special Report
January 2006
Author: Rahul Andrews
Email: rahul@ibspublishing.com

IBS Publishing Pvt Ltd
Telephone: +91 20 56030453
Fax: +91 20 56023653

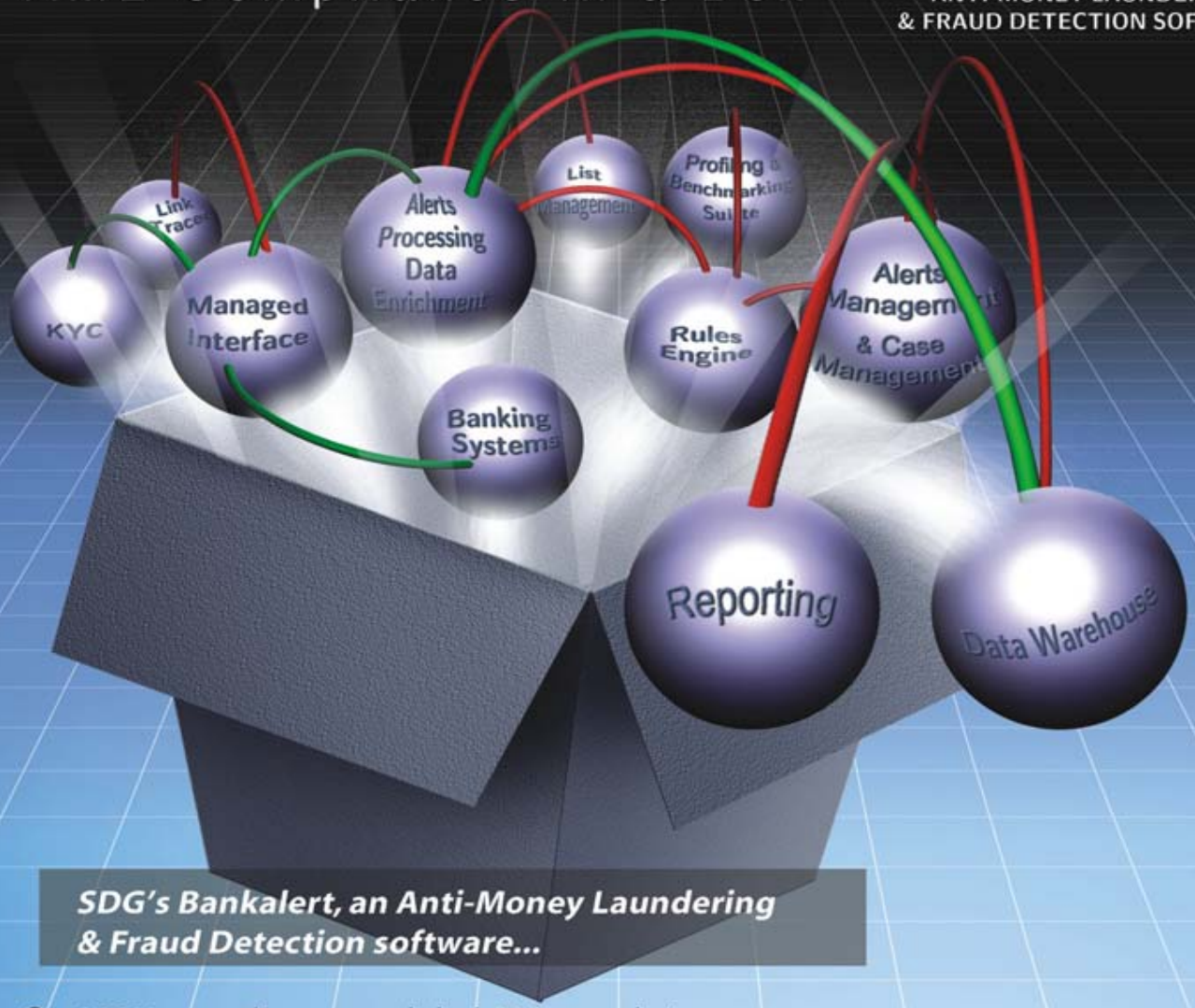
Contents

For information related to subscriptions, please email shilpa@ibspublishing.com
or write to IBS Publishing Pvt Ltd, Daya Prabha House, Gulmohar Park, ITI Road, Aundh, Pune 411007, India.

Signed, Sealed & Delivered

AML Compliance in a Box

BANKALERT
ANTI-MONEY LAUNDERING
& FRAUD DETECTION SOFTWARE



SDG's Bankalert, an Anti-Money Laundering & Fraud Detection software...

- 100% compliance to global AML regulations
- Alerts
  Transaction, Customer, Counterparty, Region, Employee, Branch based...
- Regulatory Reports
  STRs & CTRs, Exception reports...
- KYC Compliance
- Link Tracer
- Wire Messaging Check
- Entity Resolution
- False Positive Management
- Customer Due Diligence Programs
- MIS Reports
- Black List Screening

...no sweat!

SDG
SOFTWARE
TECHNOLOGIES

Delivering value

501 Babukhan's Millennium Centre
Somajiguda Hyderabad - 500 082
Tel.: +91 (40) 2337 8190 / 191
Fax: +91 (40) 5578 5489
E-mail: info@sdgsoftware.com www.sdgsoftware.com

Status of Technology Adoption

Anti-money laundering (AML) technology, no longer viewed as an esoteric one, has most bankers in India sensitised to its imperatives. This report is a sequel to our earlier report titled 'Anti-Money Laundering and India: Local Response to the Global Problem', published in August 2004; which had introduced the concepts of money laundering, global efforts to curb it through various regulatory and compliance initiatives, increased awareness on enabling technology and its providers, and a brief update on a public sector bank which had then opted for an AML solution (along with its core banking solution implementation).

This report purports to narrow focus towards updating the industry on progress in adoption of - and trends that have set in - AML technology in India, since then. Such progress and trends need to be viewed across several touch points - regulatory and compliance initiatives, responses to those initiatives by banks, strategies adopted by AML vendors, implementation challenges faced and best practices that can be adopted.

Regulatory and Compliance Imperatives

In India, most bankers are yet to perceive the adoption of AML technology as a risk mitigation tool, viewing it only as a regulatory measure that needs to be complied with. With Indian banks attempting to take banking services and operations globally, they need to review and adopt best practices prevalent in such markets.

Proactive banks aggressively competing to capture maximum wallet share of NRI funds overseas, are faced with such overseas operations requiring compliance with the law of the land where such operations are based. To illustrate an example, a branch operation in New York will find an Indian bank accountable to the Federal Reserve Bank – the regulatory authority for banks in US - in addition to the Reserve Bank of India. In response to this compliance dichotomy, most overseas operations of Indian banks have implemented AML solutions within their branches.

Costs of Non-Compliance: A Case Study

Recently, a large European bank was penalized $ 80 million for failure in ensuring compliance to AML regulations, including correspondent bank relationships.

Bank supervisory and penalty actions require it to undertake remedial action in its worldwide banking operations and to pay $80 million in penalties to U.S. federal and state regulators. The order requires improvements to the bank's global compliance and risk management systems to ensure adequate oversight, effective risk management, and full compliance with applicable U.S. laws and regulations. In addition, the Federal Reserve Board, the Financial Crimes Enforcement Network (FinCEN, the Financial Intelligence Unit of the United States), the Treasury Department's Office of Foreign Assets Control (OFAC) and other state departments assessed penalties based on findings of unsafe and unsound practices; on findings of systemic defects in the bank's internal controls to ensure compliance with U.S. anti-money laundering laws and regulations, which resulted in failures to identify, analyze, and report suspicious activity; and on findings that the bank participated in transactions that violated U.S. sanctions laws.

The U.S. Law Compliance Program requires the bank to comply with U.S. Laws, and ensure that its non-U.S. offices and affiliates do not engage in practices aimed at evading or circumventing the bank's compliance programs and controls in the United States, including measures related to compliance with cross-border payment processing procedures; and due diligence concerning customers who directly or indirectly utilize dollar clearing and other services, including advising or confirming with respect to letter of credit transactions, of the bank in the United States.

Key findings that resulted in the bank facing stringent penalties cover:

- One of the bank's overseas branches was able to develop and implement 'special procedures' for certain funds transfers, check clearing operations, and letter of credit transactions that were designed and used to circumvent the compliance systems established by the branches to ensure compliance with U.S. laws. The bank's overseas branch removed or revised the identification of the relevant parties, including modification of payment instructions on wire transfer payments such that any reference to the transaction originating entity was removed. The branches also advised a number of letters of credit issued by the entity, subsequently reissued by one of the overseas branches such that any reference to the entity was removed. The branches of the banks also advised letters of credit, for a high-risk government entity, and reissued by one of the bank's overseas branches, obscuring the origin of the entity name; resulting in a US branch clearing U.S. dollar checks for that entity. The cleared checks were submitted by one of the bank's overseas branches, arranging that the checks were not endorsed or stamped.

- The North American Regional Clearing Center of the same bank, initially operated as a captive clearing institution for funds transfers in United States dollars, subsequently marketed such services to institutions independent of the bank's branch network. As a result, more than 400 institutions independent of the bank's network held correspondent accounts with the North American Regional Clearing Center. These financial institutions utilized the network, as well as the New York Branch, primarily as a means of obtaining access to dollar clearing and settlement systems in the United States. It was deemed that the location, number, and size of financial institutions holding correspondent accounts with the North American Regional Clearing Center - and the volume of funds transfers that the North American Regional Clearing Center processed - posed a substantial risk of money laundering.

Compliance to the U.S. Bank Secrecy Act through an anti-money laundering program prescribes (1) a system of internal controls; (2) independent testing for compliance ;(3) the designation of an individual or individuals to coordinate and monitor day-to-day compliance; and (4) training of appropriate personnel.

Peer Pressure

Increasingly, correspondent banks based out of US and Europe have also increased the pressure on Indian counterparts to comply.

Most Indian banks in such correspondent relationships are likely to come under pressure to demonstrate adherence to such AML requirements. The deadline set by RBI has been

shifted from December 2005 to June 2006, in an effort to emphasize focus on AML initiatives. However, the message is clear – failure to comply can put large banks at reputation risk, and smaller banks at existence risk. From a bank's perspective, Sanjay Sharma, corporate head (information technology), IDBI, cautions, 'notwithstanding timelines prescribed by the regulator, guidelines need to be adhered to as of today'. The implication is clear - a bank in India is required to comply with regulatory directives and ensure that it is not a conduit for terrorist accounts or dealing with banned entities, even in the absence of technology. Clearly, technology is an enabler and can only be leveraged to assist the bank fulfill compliance responsibilities.

Enforcing AML in India: Financial Intelligence Unit (FIU)

The enforcement of AML measures in India comes under the purview of the Ministry of Finance. The Indian regulator, Reserve Bank of India (RBI), actively pursues banks to put in place adequate controls to curb money laundering and oversees the progress made by banks in this regard. The Prevention of Money Laundering (PML) Act - enacted as a bill in parliament in August 2005 – has been further strengthened by the establishment of Financial Intelligence Units (FIU) under the Ministry of Finance. However, FIUs are functionally best effective when networking with peer agencies globally. Internationally, the Egmont group comprises of 101 countries with recognized and operational FIUs as members, who co-operate in areas of information exchange, training and sharing of expertise. The increase in membership (up from 94 member countries in 2004) indicates units accepted during the Egmont Group 13th Plenary, Washington, June 2005. Non-members of the Egmont Group currently include China, India and Pakistan, carried forward from earlier listings.

A key component in determining the efficacy of AML systems, and their eventual success, will be the relationship between the banks and the FIU.

Know Your Customer (KYC)

The banking regulator requires banks to comply with Know Your Customer (KYC) norms outlined by it. With December 2004 as the initial deadline, most banks are yet to fully comply. While most have initiated the process, through the customer identification process, several have attempted to implement these with inadequate training to branch level staff -particularly in the absence of appropriate technology – often resulting in potential customers taking genuine business out of a bank's doors. Banks need to caution against a knee-jerk reaction to unclear policies that may result in relegation of the account opening process to a manual interface. KYC is more about capturing a customer's demography and risk profile through technology, enabling the bank analyse and determine sources of a client's funds and accordingly take an informed decision to conduct business, based on its risk appetite. A well-established KYC program can further leverage CRM applications, enabling the bank cross-sell or up-sell products and services to clients.

While an AML solution flags concerns about transacting with a potential customer, KYC norms are meant to capture optimal critical data - not necessarily in an inflexible checklist fashion. Banks will increasingly need to discern between rule based KYC vis-à-vis risk based KYC – with practical due diligence preceding non-intuitive checklists.

Responses by Banks

With only international experiences to observe, while operating within a framework of yet maturing AML measures in India, the process of implementing such solutions has undergone several iterations towards stabilizing and maturing for perceptible efficacy. However, potentially retarding the adoption and implementation of such solutions is the fact that banks have the operational discretion to choose a process for implementation – often further complicated by the absence of clean and centralized data. With guiding principles from the regulator, interpretation and implementation of these can vary across divisions in a bank. Most operations within a bank would vary in maturity levels for report generation and pattern analysis. A comparatively more mature organization may be better equipped for implementing a sophisticated AML solution, than a peer but less mature division within the same bank.

Notwithstanding such disparate organizational demography, several banks have opted for AML solutions. Vijaya Bank, the first Indian public sector bank to implement an anti money laundering solution, has been live for nearly a year. Having selected Finacle as its core banking system (CBS) and Bank Alert for AML - with Wipro as the Systems Integrator - the bank has rolled out the software across 200 branches - out of a total of 900 branches. The purview of the implementation has crossed more than 1.5 million accounts on the core banking and AML systems. The bank currently utilizes various modules of the AML application, towards leveraging required report generation.

Other early adopters of AML technology mostly comprise private sector banks, with ING Vysya and IndusInd having selected ERASE from NetEconomy. In contrast, IDBI Bank leverages an ASP based application - developed in-house, with an Oracle back-end - integrating into the bank's core banking solution, Finacle. The bank has no plan to migrate to a shrink-wrapped product as yet. Sharma of IDBI points out, 'Any AML solution requires a large amount of integration with core systems, to extract relevant data. An AML application that sits on such a core system needs to ensure minimal redundancy and mismatches'. Further, the dynamic requirements of a maturing AML environment necessitate frequent customization – often across intra-business requirements - until those requirements are frozen. It is precisely these reasons why a bank such as IDBI would rather leverage an in-house application, signifying the need for complete control in terms of resources and go-to-market time frames. Eventually, Sharma acknowledges that the bank would need to consider a standardized workflow package that facilitates case management and provides sophisticated tools for analyzing patterns.

Earlier, the efficacy of report generation meant little unless acted upon. While RBI, as the banking regulator, has effected AML policy and regulations, the onus of analysing and acting upon instances of money laundering lay with the Ministry of Finance. With the establishment of the FIU, there is no ambiguity about reporting. While dates and procedures for submission of reports have been delineated, concomitant with the evolution of processes involved has been refinement and greater clarity on such reporting requirements. Standardized set of reporting formats and mechanisms – such as through CD/ electronic formats - are required to be facilitated by the AML system in place at banks.

While suspicious transaction reports (STR) and threshold breaches are required to be report to the FIU, no reports need to be submitted to RBI. The FIU is in the process of

establishing detailed processes that banks would be required to follow. This is expected to cover

- A commentary on specifications to detect events/ activity that qualify for reporting
- Reporting frequency
- Reporting formats

At present, the FIU has prescribed filing through submission of files in specified formats on CDs. A web based reporting mechanism, leveraging appropriate case tools, can significantly reduce operational costs of compliance. Similarly, a browser based AML solution offers platform independence and flexible access. In case of a Core Banking System (CBS), since the entire Bank is expected to be on the CBS, data availability and aggregation ensure higher efficiency of an AML implementation.

With reference to AML implementation in a decentralized environment (TBA branches), the challenge lies in data integration – aggregating all branch data into a single location, so that AML analysis can be performed on aggregate customer activity, instead of using disparate sets. Also, AML analysis - if performed on isolated sets of branch information - is deprived of critical inter-connected activity, which in many instances is central to detection of potential suspicious activity. Often, integrating TBA branches to a core banking solution can pose a challenge owing to 'last mile' connectivity issues, becoming a soft target for money laundering activities.

The bank may extract information from the TBA branch system and import it into the CBS solution end-of day or at pre-determined intervals followed by a data reconciliation process.

Hanuman Tripathi
Infrasoft Technologies

Hanuman Tripathi, managing director, Infrasoft Technologies, points out that it is important for banks to discern between fraud and anti-money laundering to minimize dilution of focus. Narrower in scope when compared to fraud (whose purview extends across credit card operations, ATM transactions, limit violations, loan accounts etc.), an AML system is intended to be preventive in nature through effective KYC and diligent reporting. While systemic failure to detect instances of money laundering have no direct loss to the bank - unlike fraud where failure to stem it results in direct loss to the bank - the failure to comply with regulatory requirements can severely undermine the reputation of a bank as the onus lies on the bank to ensure diligent reporting to the regulator. Though human resource initiatives at several banks have set up a 'Head of Compliance', most large banks have yet to define the role of a Money Laundering Regulatory Officer (MLRO).

Vendor Strategies

A nascent AML technology market is seeing itself carve up between four to five large products, backed up by extensive implementation and maintenance support capabilities. Each vendor appears to have re-positioned its product and services based on individual market perceptions and experiences.

'An AML solution should be based on a 'business intelligence' driven logical data model, which seamlessly adapts to your core system and analyses data through multiple

dimensions,' advises Tripathi. Infrasoft has deployed its AML solution OmniEnterprise across 11 banks, mostly across EMEA and South East Asia. Bank Rakyat Indonesia (BRI) has 4875 branches, of which 1,040 branches have been brought under a single banking solution. OmniEnterprise was implemented across these in a span of 4 months, and has now gone live, with the strategy for the remaining branches yet under way.

In an effort to bring its OmniEnterprise AML product closer home, Infrasoft is betting on its exposure to multi-geography AML experiences across varying jurisdiction laws, coupled with indigenous experiences in implementing TBA solutions and associated data migration issues. OmniEnterprise expects to see its first AML installation in India at Canara Bank, having bid with the IBM/i-flex consortium that was selected for implementation of a core banking system. The implementation requires OmniEnterprise to be implemented in tandem with core banking solution, Flexcube, across 1000 branches initially.

Dependent on the presence of a core banking system for maximized implementation efficacy, AML vendors are increasingly aligning themselves with large system integrators as a way of entry into large banks. While BankAlert from SDG had earlier aligned with Wipro and HP, TCS is bringing its AML product FinDNA through the core banking implementation route. Last year, TCS was selected by Central Bank of India to implement its core banking solution B@NCS-24, earlier under FNS. While the core banking product is being customized for rollout, implementation of the AML product is expected to follow.

ERASE from NetEconomy is in the process of being customized for implementation by HP at Bank of Baroda's domestic and international operations. Interestingly, the product replaces Ace Software - an AML product selected by the bank earlier, but not implemented. ERASE will integrate with Finacle, the core banking solution being implemented through HP; as well as with other diverse TBA solutions - through an offline batch analysis - that reside in non-core banking system branches.

Sensing the potential to enter the market quicker with a product vendor with core banking and branch automation experiences, BankAlert recently became part of the 3i Infotech product family through the acquisition of SDG Software.

AML implementations are vulnerable to being relegated to the technology backburner, if not included in the earlier stages of core banking RFP initiatives. Often perceived as a 'compliance' requirement than a 'risk management' initiative, AML has often become a victim of the 'low cost solution' mindset– severely undermining the more expensive core banking systems in place.

While several solutions claim to be AI (artificial intelligence) ready, the AML environment in India may not yet be ready for such solutions. Tripathi suggests that a BI based solution has distinct advantages that allow an implementation to 'hit the ground running', whereas an AI driven solution is constrained by the need for historical data and a learning curve. An undeveloped AI environment can throw up false alerts, further exacerbated by the presence of TBA transactions. ' A banker's instinct needs to be enabled by technology, not replaced by AI,' says Tripathi. However, IDBI's Sharma emphasizes the eventual need for neural engines for determining sophisticated transaction patterns, beyond flagging a breach of transaction thresholds.

i-flex, the banking technology major, has a dedicated AML practice comprising consulting and development capabilities. While the supplier has an alliance with Mantas, it assists several clients develop business intelligence driven AML dashboards that integrate with

the bank's incumbent AML package. Performing intuitive analysis on business Indicators using features including metric trends, metric comparisons and value based alerting, such dashboards employ speedometers, traffic lights, heat maps, statistical charts and geographical maps to emphasize patterns.

PEP Solutions

Core AML technology vendors are increasingly relying on peripheral but niche applications to integrate with, towards providing a comprehensive AML framework. These include screening services that often address KYC requirements requiring identity of a potential client to be established through comparison with a comprehensive third party database. World-Check, Telekurs Financial and WorldCompliance are providers that offer screening services against its list of politically exposed persons and other high risk categories, better known as PEP (politically exposed persons) lists.

Are companies, corporations and other structures considered PEPs? An FATF consultation paper indicates that a PEP with 'something to hide' may choose to conceal his or her identity by using some form of corporate structure.

How does a service provider's PEP list compare against other agencies such as the UN and OFAC, who also publish a list of such politically exposed persons? The reach of organizations such as World-Check is often wider than the official agencies that publish such lists. While the UN list covers 191 member countries, World-Check's PEP list covers 230 countries. Also, such a third party database often screens against a PEP several months - and in some cases, years - in advance before the entity has been reflected in the UN or OFAC list. An early warning system such as this can often assist a bank avert transacting with such entities, well before becoming a conduit for any potentially covert operations. One of the main accused in the Bali bombing incident had been profiled on one such PEP database six months prior, under an alias, for suspected affiliations to terror organizations.

How do such PEP lists assist banks address KYC norms? One such provider, World-Check, consolidates and organises unstructured information from diverse sources into a database of highly-structured profiles of people and entities known to be of high or heightened-risk, such as terrorists, fraudsters, money launderers, politically exposed persons (PEPs), arms dealers, and sanctioned entities amongst many other categories. Not just limited to tracking and creating profiles on such entities, World-Check also gathers information on their networks and associates, where true risk often lies.

World-Check's services can be accessed online, as well as via a datafile download. While the online services allow user invoked usage, the World-Check datafile can be incorporated into a customer transaction environment such as account opening modules, core banking systems and payment gateways. Most core banking systems require a middle-ware AML/filter solution to 'plug' into, with the World-Check datafile incorporated into such an AML/filter solution rather than directly into the CBS.

Online services can be accessed through a secure website which ensures anonymity with neither a log nor an audit trail of the names being searched and screened. Such anonymity implies that the user does not have to reveal the name of clients (or prospective clients) to anyone outside its own organisation.

…continued on page 10

'Compliance is not about keeping regulators happy. Its about enabling firms to cut their losses by not doing business with companies that might harm or embarrass them… World-Check offers businesses a tool that can help prevent problem entities from becoming customers.'
Extract from the Gartner Report ' Use World-Check Now, Avoid Embarrassment Later.'

KYC RISK REDUCTION: A PROVEN SOLUTION

Banks value their reputations. Institutions with tarnished reputations will be shunned by legitimate enterprise. Having 'assisted' in the laundering of money or in terrorist financing will be severely damaging for any financial institution. The desire to reduce all avenues of operational, regulatory and reputation risk has driven financial institutions around the world to adopt ongoing enhanced AML and KYC procedures and World-Check has for the last 5 years been there to assist in this complex but rewarding task.

Originally created to provide Swiss institutions with a PEP database, World-Check is today recognised as the world's leading provider of KYC Risk Reduction Intelligence. With institutions in more than 120 countries, World-Check has a unique global perspective of these issues and what has become clear is the following:

- Banks and indeed bankers do not want to appear on the front page of any major newspaper in relation to dictators, terrorists, arms dealers, money launders or any other such individuals.
- What therefore drives most banks to carry out active KYC and PEP check is not so much their legislative requirements but rather their reputation risk.
- Management may initially see Compliance as being a non-profit making expense until they come to understand that without effective policies the bank may face multi-million dollar fines, blacklisting by regulators, loss of correspondent banking networks and even a devaluation of share prices.
- Forward thinking institutions have come to accept they have a responsibility not only to their shareholders, directors and account holders but also to society. Institutions that do not accept they have a key role to play in fighting international crime and terrorism have a hard lesson still to learn.

'When we set out in late 2000,' explains David Leppan, World-Check's founder 'our sole purpose was, on behalf of a handful of Swiss banks, to offer an '*early warning system'* at account opening. The financial community however changed dramatically post September 11th 2001, as bankers worldwide came to terms with the fact that they had no idea of who their customers were. With the global roll-out of compliance requirements, World-Check, because of its uniqueness, was chosen to assist hundreds of institutions in dramatically and immediately reducing their KYC and PEP risk.'

World-Check today serves 1,600 institutions, including 42 of the world's 50 largest banks and more than 200 regulatory, enforcement and government agencies with its global database of heightened-risk individuals and companies.

By consolidating and organising unstructured information from hundreds of thousands of worldwide sources into a database of highly structured profiles, World-Check enables institutions to automatically and regularly screen their client-base for the presence of high and heightened-risk entities. World-Check is the most comprehensive and highly structured intelligence database service available and it has proven to thousands of bankers on a daily basis that KYC checking can make a big difference.

Today it is widely accepted that KYC checking requires diligence to be carried out not only on individuals but also on companies, trusts and even corresponding banks. World-Check from early on understood this requirement and its recognised success has been partly due to the in-depth research carried out over 5 years not only to identify these individuals but to connect them to their associates and 'front companies'. Coverage within World-Check extends from terrorists, fraudsters and organised crime to 'shell banks', sanctioned entities and PEPs (Politically Exposed Persons) regardless of jurisdiction.

'A database that simply confirms a certain individual is a senior politician but which fails to reveal risk relevant information, is of little assistance in meeting the legislative requirements for KYC and PEP identification' says Mr. Leppan. 'It would however be very short sighted to simply want to comply. One needs to understand the reasoning behind KYC and PEP checking to fully understand that it makes good business sense to want to know ones customers and thereby reduce your institution's risk'.

There is no doubt of the value of World-Check's 'early warning' intelligence. On a regular basis World-Check has profiled entities up to 2 years ahead of them being added to the Bank of England Sanction list or the US OFAC list. World-Check prides itself on being ahead on the sanction-listing curve.

Never before has a company successfully taken hundreds of thousands of unstructured, open-source documents and converted them into a highly structured KYC database. Weaving the web of relationships across more than 220 countries and territories has resulted in a unique database.' Leppan says 'The continuous researching and gathering of information allows us to keep 'connecting the dots' and as the pieces of the puzzle fall into place, data becomes intelligence.'

World-Check's drive, expertise and a global team of highly motivated professionals has led to its success. On a regular basis feedback is received from bankers, lawyers and government agents on how valuable this risk reduction service is. The most frequent compliment is that World-Check's intelligence just keeps getting better and as such the financial community is able to take on its social responsibility in stopping the proceeds of crime and terrorist financing from passing through our banking system.'

'World-Check marks a critical advancement in fighting financial crime, and is an important aspect of our ongoing efforts to prevent money laundering and terrorist financing.' David Thursfield, Director Cayman Financial Reporting Authority.

Please visit www.world-check.com for more information.

…Continued from page 7

Jay Jhaveri
World-Check

Says Jay Jhaveri, director-Asia, World-Check, 'Such online PEP check lists, and other high and heightened risk categories, are updated continuously in real time, allowing the end-user to access this intelligence immediately and on a 24/7 mode. The results of such a search can be printed out, with date and time stamped, to demonstrate KYC and due diligence efforts. During the period of the contract, the user can conduct an unlimited and anonymous number of searches.'

World-Check also provides a downloadable datafile that integrates into an automated environment. As the entire process is conducted in-house at the client institution, no one from outside can see the names of clients being screened. The datafile is updated twice a day and accessed through a secured server. Updates are available through multiple formats in daily, weekly and monthly delta files. The download of the datafile is secure and tagged with a 'check sum' facility - ensuring that the downloaded datafile is identical to that at World-Check.

Does a PEP list imply that business with such entities should not be conducted? Most legislations do not prohibit financial institutions from opening accounts for PEPs. However, financial institutions have to be aware of the (PEP) risk involved and decide on dealing with such clients, based on business policy.

Challenges and Best Practices

Emphasizing the pervasive nature of an anti money laundering application within a bank, each implementation may be perceived differently by various levels of users that span the business, compliance and IT function. While business users are driven by imperatives to introduce automated processes towards minimizing errors, maximizing information transacting convenience and customer-oriented prioritization of service levels; users responsible for compliance monitoring seek intuitive yet compliant systems and processes that assess customer and transaction risk profiles, invoke alerts, and dynamic facilitation of inter/intra organization reporting. Making this happen is the responsibility of the IT function, requiring to integrate and interface disparate (or distributed) data systems, future proofing through a scalable architecture, while feeding into bank-wide enterprise marketing management and customer relationship management initiatives.

This multi-user environment throws up challenges, to which the corresponding learning curve can be distilled into replicable best practices. Based on implementation experiences within the Indian environment and globally, some perspectives are included.

Challenges

- Policy formulation for capture of required data.
- Issues relating to partial coverage of branches under Core Banking.
- Another challenge that possibly impedes the implementation of core banking solutions has been perceived by Tripathi, in terms of the possibility that over 80 percent of business is yet to come under the purview of core banking systems in public sector banks – as compared to most private sector banks having already achieved this.
- Aligning bank policies to the current regulation while adopting international best practices.
- Interface of the AML system with the Core Banking System.
- Interface of the AML system with disparate transaction based systems.

Best Practices

When considering AML implementations, since policy and implementation bear equal relevance with respect to its efficiency, coverage of policies, quality of data captured and its consolidation need to be given sufficient importance. Best practices would include–

- Invest adequate time and resources required to implement a robust AML solution. Jhaveri observes, 'As long as KYC and AML is perceived to be a mere regulatory compliance issue, senior management will be reluctant to allocate resources towards these services. As soon as banks understand that it is a risk management issue, greater resources will be allocated.'
- Well defined, unambiguous policies with respect to KYC and Customer Acceptance

- Centrally housed Customer information (both reference and transaction data), implying that the core banking network comprehensively covers all branches or alternatively, ensuring a process that integrates all data.
- Effectiveness of AML analysis - Customer Due Diligence (KYC) and transaction monitoring being core areas, are directly influenced by the quality of data that is captured by the bank's source systems. The absence of key data elements will render any AML system ineffective. It would be in the bank's interest to ensure that templates used for gathering information (e.g., account opening formats, etc) are comprehensive.
- Establishment of an independent AML cell.
- Adequate training to staff on AML processes; while educating them on repercussions of non-implementation.
- Offsite interactions between banks and financial authorities, possibly facilitated by the FIU.

  In Thailand, the FIU holds an offsite conference with participation from all financial institutions and representatives of various law enforcement agencies, in a concerted effort aimed at improving the efficacy of knowledge sharing.

Case Study: Bank Rakyat Indonesia (BRI)

Bank Rakyat Indonesia (BRI), ranks among one of the largest banks in the Asia Pacific, and is the oldest bank in Indonesia, formed in 1895. Managing assets over USD 11 Billion, the bank has 4,875 branches across Indonesia, with over 35,000 employees and approximately 39 million customer accounts. In terms of technology infrastructure, the bank has 1,050 branches on its centralised core banking architecture with over 17.5 million customer accounts online and 600 ATMs across the country.

In an effort to support international AML initiatives, including delisting itself from the FATF-GAFI list of non-cooperative countries and territories (NCCT), Indonesia has seen its banking industry aggressively adopt AML measures and solutions. Some banks, including BRI, needed to deliver regulatory and reputation risk management through the automation of its money laundering prevention controls. The solution to be deployed by the bank was required to play a key role in the bank's prevention controls through the detection of suspicious activity, recording of suspicious transactions, reporting suspicious transactions to the regulators and efficient management of information flow across the complex and large hierarchy within the organization.

The Bank required an enterprise wide anti money laundering policy, procedure – enabled by appropriate technology - to effectively counter the risk of money laundering. After extensive evaluation of several compliance solutions, the bank selected Infrasoft Technologies, an AML solution provider from India for deploying its anti money laundering solution OmniEnterprise. Meant to facilitate the deployment of an unified AML policy across the bank, the product was also required to be interfaced with multiple databases that the bank had for various businesses. The AML product interfaced with the bank's existing database to screen customer behavior, automate customer identification process and enable seamless transaction monitoring using advanced statistical analytics.

The AML functionality deployed at BRI addressed:

- Case management and Transaction Monitoring
- Customer Identification process (Interface to Bank Indonesia, BoE, OFAC database)
- SWIFT Interface (All message types i.e. MT 100/ 200/ 700/ 900 series)
- SDN Search (In addition to BI, BoE and OFAC, the system facilitated the provision to maintain the banks own list and also provides interface to non regulatory lists e.g. World-Check)
- Rules based Engine
- Know Your Customer (KYC) module
- Risk Profiling
- Automated report generation for regulatory bodies
- Complete User management
- Automated updating of SDN Lists
- Advanced statistical modeling based Transaction Pattern Analysis

BRI's efforts are part of Indonesia's industry-wide initiatives that have achieved delisting from the NCCT list. Key challenges included the need to stabilize the application for rollout across 1040 branches, and facilitate user training. Effective program management overseen by the bank saw the rollout within 4 months.

Impact on Non-banking Financial Applications

With India becoming an attractive destination for foreign investments, it is also becoming more vulnerable to inadvertently attracting the proceeds of crime. While banks are targeted for use as a conduit for such slush funds, peripheral entities are often facilitators for money laundering operations. Some transaction originating points that may possibly come under the purview of AML systems include money changers, brokerages and securities firms and Trusts.

AMC (Money Changers)

In December 2005, RBI issued guidelines, including KYC processes, which spelt out procedures that AMCs are required to adopt in detecting potential instances of money laundering.

Brokerages and Securities Trading Firms

In January, it was estimated that NRI funds in excess of $ 20 billion were being channeled to India towards investment in the economy. With concerns raised about the quality and source of investments pouring into the country, participatory notes (PN) have invited criticism. Implementation of KYC norms requiring disclosure of sources of funds is likely to institute checks and balances to an extent.

Some sources from the industry hint at the need for brokerages and securities firms to come under the scope of AML regulations, as these are potential transaction capturing points– or executors - for bad money, while banks may only be limited to acting as a conduit. The recent IPO scam is possibly an indication of the buy-side money laundering efforts.

Trusts

Trusts that manage funds are also likely targets for money laundering, in the absence of regulation.

Indonesia, now aggressively combating money laundering operations beyond banks, is expected to empower its anti-money laundering watchdog, Financial Transaction Reports Analysis Center (PPATK), along these lines. Based on annual statistics attributed to PPATK, 3311 reports of suspicious transactions (STR) were lodged by 106 banks and 26 non-bank institutions at the end of last year, up from 1,256 STRs by 69 banks and 10 non-bank institutions recorded the previous year.

A proposed revision of Law No. 25/2005, article 59, on money laundering, could see PPATK taking over the investigation of cases from the police as well as freezing assets and halting financial transactions linked to money-laundering. Non-bank institutions such as public accountants, real-estate developers and agents, jewellery and antique shops, car dealers, lawyers and non-governmental organizations (NGOs) would be required to report suspicious transactions to the regulator. Such transactions are amenable to getting postponed by authorities, bringing administrative sanctions on those who fail to report them. The proposed changes were based on the recommendations made by the Financial Action Task Force (FATF), the global anti-money laundering watchdog that removed Indonesia from the list of Non-Cooperative Countries and Territories (NCCT) in February

last year. Currently on a monitored status, FATF will review Indonesia's position in its plenary session in Cape Town, South Africa, in February to decide whether the country can be taken off the list.

OUR VISION

Our vision is to assist in the evolution of the banking technology market

About IBS Intelligence

IBS Intelligence is the management consulting arm of IBS Publishing, building on over fourteen years of unparalleled knowledge of the users and suppliers of core banking solutions. Our clients include:

- Banks undertaking system selection exercises;
- Research analysts and investors who seek to better understand the market and its players; and
- Vendors who wish to re-align their corporate and product strategies to meet market expectations.

We have borne witness to the mistakes and the masterstrokes and bring with us the unrivalled advantage of witnessing and recording the strategies that work for our clients. Our commitment is to use this knowledge to help our clients create a significant impact on their performance.

For further information on IBS Intelligence, contact

Shirish Pathak
Director
Tel: +91 20 56030453
Email: shirish@ibspublishing.com
Website: www.ibsintelligence.com

Indian Banks' Association

About Indian Banks' Association

The Indian Banks' Association, formed in 1946, is an advisory service organisation of banks in India. It serves as a co-ordinating agency and a forum for its 156 member banks to interact in matters concerning the banking industry.

For further information, contact

Rema K. Menon
Vice President (Technology)
Telephone: +91-22-2218-2196
Email: rema@iba.org.in
Website: www.iba.org.in

You don't buy a puppy to guard your house !

Then, why deploy a low cost, unproven AML software to guard your bank ??

Take a look at this real life scenario which is now happening around you ...

Some of the Banks where they opened accounts already had an AML solution in place... Others did not even have one...

Your investment in a bluechip core banking solution gets nullified with poor compliance & regulatory reporting peripherals.

Choose OMNIEnterprise™ anti money laundering

1. Business Intelligence based transaction monitoring that is close to how your banking instincts work....high accuracy in identifying the "truly suspicious", without disturbing the clean customers

2. Comprehensive KYC with Link Analysis, Identification process and Risk based profiling, to ensure pre-emption rather then just cure

3. Ready solution not just for banks but for the financial world....Insurance, Mutual funds, Wealth Managers, Brokerages and Money Exchangers... or even one enterprise having all of these businesses

4. Ready with multi-geography Compliance & Regulatory reporting... single solution for your global operations

OMNIEnterprise AML is the fastest growing and most widely accepted solution globally, with 12 sites gone live in 18 months; with one of the largest sites in the world to our credit.

InfrasoftTech has built the AML solution using decade long experience in delivering technology for enterprise banking to 100 financial enterprises globally. We understand your AML deployment & integration the best, to ensure complete & timely implementation.

Right Technology...Most Proven Solution...Most Reliable Partner

InfrasoftTech

www.infrasofttech.com

Global Marketing Team:
Mumbai: +91 22 5649 2222 Fax:+91 22 5649 2233, email:corporate@infrasofttech.com
London: +44 20 76655444 Fax: +44 20 76655440, email:london@infrasofttech.com
New York: +1 212 292 5007 Fax: +1 212 292 5014, email:newyork@infrasofttech.com
Middle East: + 971 50 6513375, email:middleeast@infrasofttech.com