

Understanding the Role of Technology in Anti-Money Laundering Compliance

In an effort to detect potential money laundering schemes, many financial institutions have deployed anti-money laundering (AML) detection solutions and enterprise-wide procedural programs. These solutions worked by establishing fixed rules-based monetary thresholds and detecting specific money laundering patterns and user scenarios that breached those thresholds. As new schemes were developed, many of these “first generation” solutions were unable to uncover them, providing criminals with new avenues to circumvent detection and the law.

Today there is a perceived need on the part of financial institutions to take these capabilities to a higher level in order to address the shortcomings inherent with first generation solutions. As a result, a “second” generation of AML technologies has emerged with the ability to monitor every single transaction, discover various types of unusual behaviors, and alert officials to the activities that represent true risk to the financial enterprise. These “intelligent enterprise system” are able to learn and adapt, comprehending new money laundering schemes as they arise. With their enterprise-wide approach, they are able to analyze both the client profile and all of the transactions that are undertaken by them, helping the financial intuitions prevent money laundering schemes in a much more effective and efficient manner.

These second generation anti-money laundering systems are comprised of four key risk assessment components:

- **Client Risk Assessment** – Using detailed information and transaction activities which are collected at the time that an account is opened, to investigate all aspects of the customer’s profile.
- **Transaction Risk Measurement** – Identifying and filtering account-related transactions that pose the greatest risk for potential money laundering activities.
- **Behavior Detection Technology** – Using specific technologies that are able to detect suspicious patterns of behavior that may be hidden beneath large volumes of financial data.
- **Workflow and Reporting Tools** – Using tools that will assist in alert investigation and compliance reporting.

By analyzing financial data in this fashion ! second generation AML solutions allow the financial establishment to deter potential money launderers before they are able to proceed, providing protection in the form of full compliance with these new regulations. These second generation solutions should be strongly considered as part of a strategic anti-money laundering technology plan within today’s financial organizations.

Introduction

The term “money laundering” has been a part of the modern lexicon since the time of American gangsterism that arose out of the Prohibition Era of the late 1920’s. At that time, several discreet mechanisms were used to disguise the original of large amounts of money that were generated through various illegal racketeering operations.

Today, money laundering has become a key funding mechanism for international religious extremism and drug trafficking, and curtailing these illegal activities has become an important focus of the U.S. government as part of its ongoing wars on drug abuse. According to one estimate, the amount of illicit funds traveling through money laundering channels was expected to reach over \$900 billion worldwide by the end of 2005, and grow at an annual rate of nearly 3% As of figures compiled during 2002, the largest region for this traffic came from North America representing 28 percent of total worldwide money laundering traffic.

To assist law enforcement agencies, the U.S. Patriot Act became law in October 2001 and with it a provision was included entitled Title 111 that froze the U.S. based assets of any suspected organizations and individuals involved in money laundering with the goal of “starving” terrorist networks. The act, which Congress strengthened after the terrorist attacks of Sept, 11, 2001, requires financial institutions to alert law enforcement officials to unusual banking activity that might be deemed suspicious. In addition, it grants the Treasury Department with regulatory powers to penalize any U.S. financial institution that might participate in these schemes, whether knowingly or not.

Beyond the detailed process of uncovering these schemes is the pressure that will result the form of federal compliance. Failure to meet these stringent anti-money laundering (AML) regulations or to allow suspicious transactions to go undetected can have a severe impact on any financial entity, including damage to its reputation, market capitalization, as well as its customer perception and loyalty.

Riggs Bank agreed to pay \$25 million in civil penalties for what federal regulators called a "willful, systemic" violation of the Patriot Act's anti-money-laundering law.

The New York Times, July 20, 2004

An excellent example is that of Riggs Banks. Riggs, which for years billed itself as "the most important bank in the most important city in the world", found itself in a precarious position as one of the most scrutinized banks in the financial community. After a two year FBI investigation, the U.S. Senate's Permanent Subcommittee on Investigations concluded that Riggs executives and bank regulators "failed to monitor suspicious financial transactions involving hundreds of millions of dollars", The ruling came a day after Riggs Banks agreed to pay \$25 million in civil penalties for what federal regulators called a "willful, systemic" violation of the Patriot Act's anti-money-laundering law.

Detecting a potential money laundering scheme, combined with the threat of reputation damage for lax compliance as with the case of Riggs Bank, have caused many financial institutions to revisit their existing anti-money laundering solutions and prevention measures.

In order for financial institutions to manage all of the intricacies involved with the issue, the implementation of new software solutions will be required that relies on sophisticated behavior detection techniques to correctly assess an organization's current level of risk exposure, and ensure complete regulatory compliance for all of their financial operations.

Before the benefits associated with these new software solutions can be appreciated, financial institutions need to understand and re-evaluate the areas where their current AML solutions have not been able to keep up with existing money laundering schemes.

The shortcomings associated with first generation AML solutions

First generation enterprise-wide AML detection solutions have been a part of the financial community for a long time. These solutions work by establishing a fixed rules-based threshold by analyzing how certain established usage scenarios comply within those boundaries. Most financial institutions will establish a threshold based on a set monetary value for each transaction, flagging any transactions over a certain monetary level, such as those over \$10,000. There are three areas where first generation AML solutions have had difficulty detecting money laundering schemes include:

- **Transactions Below Defined Thresholds** – First generation solutions have an inherent inability to detect money laundering schemes of smaller amounts that may come in under an established threshold limit. For example; money launderers will make several smaller deposits into several individual accounts, and then at a later time, aggregate those funds into a single larger account.
- **False Positives** – These are transactions over a set limit that are marked as suspicious but that do not represent any existing identified risk to the institution. Securing a mortgage, for example, could represent any existing identified risk to the institution. Securing a mortgage, for example, could represent a transaction that is of an unusual size for an existing account, but is also legitimate and does not pose a risk. The problem with false positives is that they can easily overwhelm a financial institution by dedicating many resources to the investigation process while taking the focus off of other transactions that might be more representative of a true money laundering risk.
- **Behavior Profiling** – This is defined as the process where current industry information is used to profile and confirm certain patterns of suspicious laundering activity. In one case, a business account for a pizzeria was set up to launder money. The restaurant seemed to have

consistently high sales throughout the year with no lulls or exceptionally busy periods. By comparing the pizzeria's transactions against an industry peer group, the account suddenly appeared very suspicious. While similar pizza restaurants experienced a dip in sales just after the Christmas holiday, the targeted restaurant did not have that downturn during that same timeframe. In this instance, adaptive profiling enabled the financial institution in unearthing the money laundering scheme.

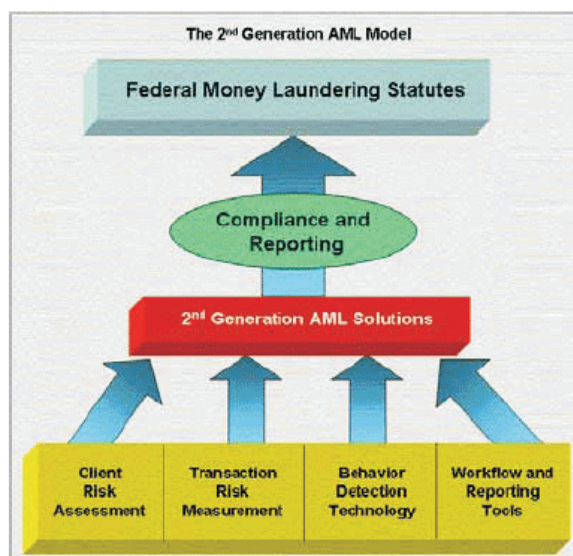
The federal regulations required for detecting money laundering demand more sophisticated information system that will generate knowledge of the customer, their financial standing and account-related activities.

How New Technologies Assist in the AML Process

The value of any AML solution has to be based on its ability to uncover suspicious financial activities by identifying the specific individuals or organizations that may be involved.

A second generations of AML technologies has emerged that provides the ability to monitor every single financial transaction, discovering all unusual behavior, and separating out those transactions that are determined to represent a true risk for the financial enterprise. These "intelligent enterprise systems" are able to learn and adapt, comprehending new money laundering schemes as they arise. They take an enterprise-wide approach, determining every transaction that is unusual as opposed to looking for a specific patterns or behavior while analyzing both the client profile and the transactions undertaken by the financial firm.

Second generations anti-money laundering systems are made up of four basic risk assessment components that ensure full disclosure and reporting necessary for compliance with the federal statutes:



- **Client Risk Assessment** – Using detailed customer profiles for investigative purposes.
- **Transaction Risk Measurement** – Identifying transactions with the greatest risks.
- **Behavior Detection Technology** – Recognizing suspicious patterns of business behavior.
- **Workflow and Reporting Tools** – Tools that assist in alert investigation and compliance reporting.

Client Risk Assessment

Central to the process of uncovering a money laundering scheme is the ability to access a wide variety of detailed information relating to the customer's account, typically collected at the time that the account is opened. Second generations AML systems differ from their predecessors by providing a single view of the customer profile incorporating all of the various financial relationships that the account has an affiliation with. The types of analytical activities that are part of second generation client profiling processes include, but are not limited to:

- **Watch List Name Screening** – Besides the name(s) of the principal account holder(s), client accounts can also include the names of other individuals or organizations that are affiliated with the account such as the beneficiaries, Power of Attorney holders, Trustees, etc. The system will screen these names against the various watch lists published by watchdog agencies such as OFAC, Bank of England, and the FBI, among others; several

vendors like Thomson Financial and Equifax also provide periodically updated information which can also serve the purpose of a watch list. The watch lists that are chosen would be driven by the regulatory needs in the various markets from which the financial firm operates.

- **Country Alerting** – High risk countries that are associated with a particular account, such as wire-transfer transactions, can be flagged for further investigations obtained through the Financial Action Task (FATF). FATF classifies all countries into four tiers, relating to their compliance with U.S. AML regulations (Tier 1 for example, represents the highest level of compliance). Example of country-related information that can be used by second generation AML systems include: country of residence, nationality of the account holder, and tax domicile.
- **Channels** – The channels that are used by the account holder can include information on the financial representative of the account, the locations of the branch office(s) that are used for transactions, and point-of-origin information pertaining to the online banking activities of the account holder.
- **Business Relationships** – Business affiliations serve as an additional profiling criteria and include the name and numbers of business relationships that are associated with the client account, as well as the numbers of years since each of those relationships were first established.
- **Political Affiliation** – Customers occupying political offices may pose a greater risk for money laundering, and as a result, would require closer scrutiny as part of a client profile since they could be a source of funds from questionable foreign origins.

Transaction Risk Measurement

Another critical element of second generation AML systems is their ability to identify transactions that pose the greatest risk for potential money laundering activities. Transactions determined to be of a higher risk can vary from organization to organization based on their lines and type of business. For example, the risks associated with transactions from a bank would be different from those associated with an insurance agency or a securities firm. These transactions fall into one of three categories:



- **Fund Related Behaviors** – Transactions that generate receipts into the firm and/or payments made by the firm. These include internal transfers between accounts, rapid movement of funds in or out of the account, or sudden activity into a previously dormant account.
- **Transaction Related Behaviors** – Behaviors where transaction values fall above specified limits and are apart from established internal guidelines that can pose additionally higher levels of suspicious activity and risk of money laundering, which are typically flagged for further investigation.
- **Miscellaneous Behaviors** – Frequent changes to an account can often be a signal that money laundering is taking place. Activities that would fall into this category include the settlement and/or standing instructions of an account, the movement of funds without a corresponding trade, and the deposit of excess collateral into an account. These types of offsetting trades can increase the potential for risk of money laundering, as in the case of a stock that has buy and sell dates with very short periods of time between them.

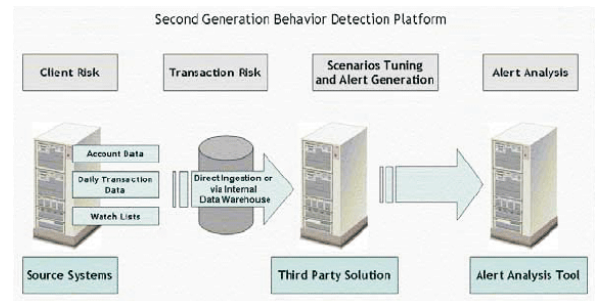
Behavior Detection Technology

Behavior detection technology is another important aspect of a second generation AML system. This function manages the complex behavior that is commonly associated with money laundering schemes. This technology allows financial firms to detect wrongdoing by finding suspicious patterns of behavior that may be

hidden behind large volumes of financial data. The key to behavior detection technology is its ability to identify suspicious events and entities that build over time, thereby separating them from normal every day events and transactions in order to target the offending behavior. The technical terminologies relating to the components that contained within the behavior Detection section of a second generation AML solution include:

- **Scenarios** – Scenarios are the patterns of behavior that are of interest to the organization and form the basis for a new generation of AML surveillance. A scenario is nothing but a combination of rules and/or conditions which define the transaction pattern that is being detected. For example, wire transfer receipts from high risk countries would involve detecting the country code associated with an incoming wire and examining it if it corresponds to a high risk /low risk country.
- **Thresholds** – Thresholds are the triggers that first inform officials to potential fraud scenarios. Thresholds are defined for those data elements that are relevant to a particular scenario or pattern. Thresholds are extremely useful in elimination of false positives and ensure that only the most relevant results will be reported.
- **Alerts** – The discovery of actual fraud scenarios are referred to as “alerts”. As the name indicates, its function is to alert the user to any possible matches of potential money laundering fraud which subsequent investigations will then be required. These investigations could result in either the alert being closed (as in the case of a “false positive”) or for escalation to additional steps such as further investigation, corrective action, and/or the reporting of the instance to the appropriate authorities.
- **Look Back Period and its Frequency** – “Look back period” is the length of time monitored for a scenario in each run of the detection process. This could vary from a day to 12 months depending on type of behavior that is being monitored. ‘Frequency’ defines the periodicity of running a given scenario eg: daily, weekly, monthly etc. Selection of the appropriate frequency parameter is important to ensure that duplicate alerts are not generated for a given scenario.

These components can be broadly categorized into three sections, which are illustrated in the diagram below:



- **Source Systems** – Source systems provide the inputs for the transaction surveillance platform. These would include account and transaction data, client risk profiling information and watch lists against which name matching of counterparties could be carried out.
- **Behavior Detection Platform** – This would normally be a third party product such as solutions from Mantas, search space, or SAS.
- **Alert Analysis Tools** – The alerts that are generated are transferred into these systems for further investigation using the Workflow and Reporting Tools that are identified in the next section.

Workflow and Reporting Tools

As we have already established, complying with external rules and regulations is now an essential component for any financial institution. Those that remain fully compliant have an advantage by shielding themselves from any negative legal or public relations exposure. Since customers prefer to work with companies that fall in line with the regulations, financial institutions that remain complaint are in a position to gain greater customer visibility and loyalty.

However, it is not unimaginable that in spite of the best checks and balances that may be already in place, financial entities may inadvertently fail to comply with a minute proviso or a sub regulation .In such a case, the existence of an effective compliance system that is able to provide verification would satisfy federal regulators and could prove to be a mitigating factor in preventing any subsequent liability or violation.

Second generation AML solutions provide financial institutions with several tools that aid in the workflow and reporting process, which are essential in regulatory compliance. These tools include:

- **Case Management** – Most platform provide an alert analysis workflow that is integrated with basic compliance reporting tools. Alerts that are generated from second generation AML solutions are pumped into these tools for further investigation. Organizations may choose to adopt or integrate these into existing case management systems that may have been modified for the necessary compliance programs.
- **Record Keeping** – The ability to remain in compliance with federal laws requires that financial institutions are able to preserve their records for specified periods of time. Since the volume of these records can be quire extensive, a compliance software solution provides scanning, imaging, indexing and electronic storage of the physical transaction documents. When a particular record or series of records are required for a compliance review, the software provides easy accessibility and retrieval of the information. Also, automated workflow and case management tools cam also be included that provide additional layers of information that can compliment and assist the investigation and reporting process.
- **Reporting** – Reporting capabilities are an add-on feature for both the transaction monitoring and watch list filtering solutions that generate Suspicious Activity/Entity reports, currency Transaction Reports (CTRs) and any other customized reports for internal stakeholders or federal regulators.

Concluding Summary

Criminal elements in today's technology-driven society are using every means available at their disposal to launder the proceeds from their illegal activities. Now that governments are using a host of counter-intelligence resources in an effort to thwart these activities, they are also leveraging their legal resources to ensure that the financial community is able to assist them in their investigative efforts. Failure for any financial institution to ensure full compliance with these new laws can result in stiff financial, public relations, and customer satisfaction-related penalties.

While many anti-money laundering (AML) solutions have been in place for some time within the financial community, the efficiently by which these older AML solutions were able to detect, alert, and prevent potential money laundering schemes was dependent on the quality to the data collected by the financial institution, and the capabilities of the tools that are tasked with analyzing that data.

The second generation AML solutions that are now available provide a superior means of detecting new money laundering schemes. These solutions go beyond earlier systems by completely analyzing all related financial data in a greater level of detail by scrutinizing smaller transactions and profiling and detecting account behaviors. This minimizes transaction risks ensuring full compliance with federal money laundering regulations. These newer solutions should be strongly considered as a vital part of any strategic anti-money laundering plan that is part of the financial information infrastructure.

Authors

Rajesh Menon

Sr. Consultant
Infosys Technologies Ltd.

Sanjaya

Sr. Consultant
Infosys Technologies Ltd.



Infosys Technologies Limited, Plot No. 44, Electronics City, Hosur Road, Bangalore - 560100. India • Tel.: +91 80 28520261 • Fax: +91 80 28521747
e-mail: finaclemtg@infosys.com • www.infosys.com/finacle

"COPYRIGHT NOTICE: Copyright ©2009 Infosys Technologies Limited, Bangalore, India. ALL RIGHTS RESERVED." Finacle logo is a registered trademark of Infosys and Infosys acknowledges the proprietary rights of the trademarks and product names of other companies mentioned in this document. Infosys believes the information in this publication is accurate as of its publication date; such information is subject to change without notice.