

METAVANTE WHITE PAPER

Evaluating AML Technology to Achieve Compliance Efficiency

David DeMartino

Vice President, Prime Associates (a Metavante Company)

Tony Kaus

Metavante Risk Management Consulting



1-800-822-6758

Table of Contents

Coping with Today's Stringent AML Compliance

Technology as a Solution

Surveying the AML Solutions Landscape

Manual Reports

Advanced Software Technology

The 'Hybrid' Solution

Evaluating AML Technology Effectiveness

Optimization and Multiple Constraints

The Importance of Effective Software Development

Summarizing Effective AML Technology

The Right Vendor and the Right Technology



1-800-822-6758

Coping with Today's Stringent AML Compliance

Until shortly after September 11, 2001, a banker's approach to anti-money laundering (AML) was to focus on putting together a compliant Bank Secrecy Act (BSA) program that could be documented. In those days, the thrust of BSA investigative work wasn't money laundering so much as the detection and prevention of fraud, particularly tax fraud, by keeping an eye on large cash transactions and making sure they were reported correctly to the IRS. Compliance amounted to little more than the checking off of boxes on an AML procedural worksheet.

This approach changed radically with the onset of the USA PATRIOT Act, which greatly expanded obligations that were part of the AML regulatory process.¹ To date, the increasing scope of accountability has proven extremely challenging for financial institutions, compounded by the large up-tick in activity that banks are expected to monitor—specifically, money laundering schemes and review of account relationships, account risks, and transaction activity. There is also a new focus on the monitoring of domestic and international transactions and the parties to those transactions. Private banking, correspondent activity, and customers with international ties also require specific scrutiny. The fourth and latest (as of the time of this writing) issue of *The SAR Activity Review—by the Numbers* (May 2005)² illustrates this increased scope by documenting the rapid increase of Suspicious Activity Report (SAR) filings:

Number of Suspicious Activity Report Filings by Year									
Form	1996	1997	1998	1999	2000	2001	2002	2003	2004
Depository Institution	32,069	81,197	96,321	120,505	162,720	203,538	273,823	288,343	381,671
Money Services Business	-	-	-	-	-	-	5,723	209,512	296,284
Casinos and Card Clubs	85	45	557	436	464	1,377	1,827	5,095	5,754
Securities & Futures Industries	-	-	-	-	-	-	-	4,267	5,705
Subtotal	52,154	81,242	97,078	120,941	163,184	204,915	281,373	507,217	689,414
Total	2,197,518								

Figure 1. SAR filings by year, 1996 – 2004

The report summarizes key aspects of the above activity as follows:

- Between April 1996 and December 31, 2004, 1,660,387 Suspicious Activity Reports were filed
- The volume of Suspicious Activity Report filings in 2004 increased 32% over those filed in 2003
- BSA/Structuring/Money Laundering continued to be the leading characterization of suspicious activity filed by depository institutions
- Identity theft was added as a suspicious activity characterization in July 2003. In 2004, 15,491 Suspicious Activity Reports were filed with this characterization box marked
- Mortgage Loan Fraud increased 93% since 2003
- Computer Intrusion decreased 59% since 2003
- Debit Card Fraud increased 70% since 2003

The depth (frequency) and breadth (variations) of AML-related activity contribute to a challenging complexity. Unlike fraud losses, there is no way to be certain that money laundering has occurred because losses do not appear until 60 or 90 days after an event and there is no other red flag (unless you count those situations in which an institution finds itself in the headlines due to some activity uncovered through law enforcement efforts). Most often there is not even a follow-up or response to filed SARs. There are such a wide number of variables to consider, it is impossible to effectively anticipate all potential outcomes. Plus, all of this can be even more challenging in those instances involving employee misbehavior when the embarrassment factor is exponentially increased.

¹ A detailed look at evolving AML obligations, including their nature and background, can be found in *Meeting the Challenges of AML Compliance: Consulting Solutions Using a Holistic Approach*, by John Hurlock, a Metavante White Paper available at www.metavante.com.

² This document is published by the Financial Crimes Enforcement Network (FinCEN) of the United States Department of the Treasury and is available, in full, at www.fincen.gov.

Technology as a Solution

To help individuals cope with these AML-related developments, banks are looking to technology with robust analytics to help identify transgressions in a timely manner, prevent them in the future, and provide at-hand proof of their efforts at the request of regulators, who are now suggesting that compliance technology and automation is readily available and affordable for banks of all sizes. This provides an increased impetus for banks with more than a few hundred million in assets, large credit unions, and other financial services providers to search for automated AML tools and processes.³

It's not an easy task. Literally dozens of solutions employing various technology levels and flavors have emerged in the financial services marketplace. Individuals within the bank – often a financial officer used to evaluate purchases with ROI formulas – may not have the necessary background to evaluate potential solutions, clouding the mission at hand to an even greater degree. How much technology is enough? How can it be implemented? What is a reasonable investment? What results are deemed acceptable and what can be realistically expected? What resources does an institution have or need to implement, maintain and optimally use AML software technology?

With so much at stake, banks cannot afford to take an intuitive, superficial, or other less than effective approach (such as using traditional models for ROI) in their search for the right AML technology fit. Although the market is rife with those who have, these individuals have ended up with a white elephant on their hands as a result (not to mention unabated and sometimes increased AML exposure). Because the failure of such a system is, many times, not immediately apparent, the problem is exacerbated. It likewise should be pointed out that the most notable AML failures have been due to implementation issues rather than the technology itself.

This doesn't have to be the case. While many resources can shape this decision making, such as the financial

institution's regulatory agency, industry peers, professional associations, third-party financial services providers, and consultants from a variety of professional segments, it is ultimately the bank's responsibility to educate itself. Fortunately, there exist guidelines and a strategic approach consisting of concrete methodologies that can help decision makers make a prudent, effective choice.

Surveying the AML Solutions Landscape

The foundation of an intelligent purchase is the fundamental understanding of choices, how they differ from each other, and which integrate best into a particular organization. Assessing the AML solutions landscape is a process that often begins with a solicitation of regulator opinion. This can be somewhat problematic given that regulators cannot appear to endorse specific products. A discussion with trusted peers or financial institutions willing to share their approach is a possible second step, and a third is the obtaining of information from professional organizations' leading industry publications and reports from industry analysts.

There are limitations to the method. Peer and industry opinion exerts such a strong pull on bankers that uninformed hearsay is often accepted to the detriment of due diligence. Additionally, a majority of financial institutions – at least at this point in time – tend to favor their judgment of AML technologies with an inordinate amount of emphasis on cost and traditional ROI models when a more progressive analysis is needed. There is no substitute for the financial institution itself carrying out the lion's share of a detailed and in-depth investigation, as it is in the best position to determine how a technology might address its AML compliance needs (assuming it follows a best practices approach in analyzing processes and procedures.) This is mainly because it has (or should have) an unparalleled understanding of its own

risk categories and tolerances as well as its business, operational, and technical requirements.

3 Though important, asset size is not the only or always the best indicator for AML technology needs. Geography, business activities and other types of risk categories should also be considered

Manual Reports

When it comes to identifying potentially suspicious activities, manual reports are the least sophisticated way to deliver data. This is because reports provide straightforward information such as the highest volume events, or events in excess of some set threshold. Plus, a number of different reports are used. These include data taken directly from bank applications, ad hoc or predetermined database queries, or use of a variety of third-party report-writer-based tools. These are typically based on requirements defined by various bank personnel, as well as report transactions or account information detail in a linear fashion, that is, on a first-in first-out basis. Some report generation may employ basic logic conditions such as aggregation of events within an account and sometimes between related accounts.

Reports are delivered to the user for a manual review of these linear events, leaving analysis to subjective and variable conditions based on the recipient of the report. It is estimated that in today's environment 10 percent of U.S. financial institutions effectively meet their compliance needs by adopting this approach.

Advanced Software Technology

These are "high end" solutions that monitor large amounts of data using "targeted" algorithms and advanced heuristics often tailored to the specifics of the institution. Initially offered by a handful of providers, the market has evolved so that one major vendor is the virtual lone supplier of this type of system. A high-end solution takes a data mining approach requiring vast amounts of information, and

uses it to monitor suspicious relationships and predefined event patterns. Approximately 10 percent of the largest U.S. financial institutions are likely candidates for this option.

The high-volume/high-tech solution requires a significant investment in terms of implementation, hardware, software licensing, maintenance fees, and personnel (to support ongoing use). It is labor-intensive to implement and is relatively inflexible in terms of ongoing modifications, almost all of which would require vendor support. Its complexity makes it difficult for a bank to "swallow" in one gulp.

The 'Hybrid' Solution

The hybrid solution consists of a variety of technology-based software applications that incorporate rules, conditional logic, computational techniques, math-based analytics, and statistical metrics. This solution requires less investment and implementation than the high-end solution, and its operation and maintenance are not as labor intensive. It contains an element of flexibility missing from the high-end approach, therefore, users are often able to adjust numeric values such as thresholds and risk scores in addition to accessing other settings. This is a viable alternative for 80 percent of U.S. financial institutions and the majority of financial services companies. Additionally, there are many instances where the deployment of the advanced software technology solution could be augmented by the supplemental use of a hybrid solution, as there are often capabilities in the hybrid solution that meet specific functionality needs often unavailable in the "high end" data mining implementations.

Worthy hybrid solutions address three capabilities that form the baseline for AML technology effectiveness, including:

- Transaction monitoring – the scanning and analyzing of data in transactions and other account information to identify potential money laundering activity
- Watch list filtering – the screening of new accounts, existing customers, beneficiaries and transaction

counterparties against terrorist, criminal, and other blocked-persons or persons of interest watch lists published by various organizations and government agencies

- Automation of audit trail requirements and regulatory reporting -- this encompasses data management and the filing of suspicious activity reports (SARs) and currency transaction reports (CTRs) with the appropriate authorities. This provides centralization of all relevant AML information and tools to keep the user’s management team and the institution’s Board of Directors apprised of compliance activities and events

Some hybrid vendors offer the capability to score customers at the time of account opening and track ongoing risk scores through ongoing activity monitoring. This may soon become a fourth baseline requirement for compliance, and many feel it already has.

There are other capabilities that may become commonly expected by regulators and users that are provided by a hybrid solution. These include customer profiling as well as peer-to-peer comparisons for behavior not consistent with the rest of a measured group. Information such as NAICS (North American Industry Classification System), SIC (Standard Industrial Classification), and ZIP codes can be useful data points for monitoring potential suspicious activity in peer groups.

Properly deployed, the suite of tools that makes up the hybrid solution are most suitable to effectively monitor the four Vs of money laundering: *Volume* (a reference to event activity levels); *Velocity* (monitoring money moving in and out of an account or account relationship); *Value* (looking at the amounts involved in current transactions); and *Variance* (behavioral changes: a structured form of monitoring across data with accounts, account relationships, products, channels, and other categories specific to the user’s environment). These tools form the basis for hybrid solution use, as illustrated in Figure 2.

	Rules	Statistics	Analytics	Proprietary Approaches
Volume	Exceeds "X" Trnx's in "Y" days	Exceeds Average # of Trnx's in Acct	Exceeds Total Item Count Across Related Accts	Analysis to Compare Account Activity to Similar Accts (Peers)
Velocity	Debit and/or Credit Counts	Standard Deviation for # Days Acct Balance Maintained	Average Collected Balance as a Percent of Debits & Credits	Evaluation of Acct Balances to all Other Accts in a Category
Value	Cash Trnx Amount(s) Exceed \$10,000	Setting of Threshold for High Debit in Terms of top %	High Debit Exceeds High Debit for Acct Type	Techniques to Monitor Aggregated Amounts between Accounts
Variance	Change in Account Behavior Such as Increased Activity	Acct Activity Differs by More than "X%" Over Variances that Occurred in the Past	Compared to all Accts in a Specific Geographic Area Behavior is Different	Profile for an Acct's Activity Looks Similar to Profile for Money Laundering

The contention of this paper is that the hybrid solution is the best level of technology available for financial services providers to address today’s AML compliance needs. It provides the desired functionality and flexibility to adapt to users’ needs not only during installation, but over time as the user’s environment and needs change as files are modified and percentage thresholds and other settings changed. In some instances rules may even be added, contributing to an application that evolves over time with or without user approval and/or intervention.

Evaluating AML Technology Effectiveness

Once an AML technology level has been selected, available solutions within the category—in-house or vendor supplied—must be evaluated. Given the problem’s complexity, it is most likely that only a manual report process would be developed in-house.



As mentioned previously, solutions falling under the hybrid umbrella provide a wide range of functionality. These include the ability to dynamically change the assessment metrics used at the account and relationship levels; robust case management for tracking cases and events related to cases; provision of a central repository for all AML data; added effectiveness through automatically and/or manually assigning tasks; an ability to relate case events together over time; and many others. Hybrid technology is scalable, secure and modifiable, providing significant advantages over the alternatives.

Unfortunately, AML applications are often thought of in the same terms as fraud applications, so the same standards used to evaluate fraud software end up being erroneously applied to AML software evaluation.

Among these fallacious comparisons, the most notable is the alert rate, which is the false positive rate associated with it (see the above sidebar for a discussion of false positives and related concepts). Another concept wrongly applied to AML software evaluation is the attempt to determine a calculable ROI for the system to determine whether or not to invest in it. This technique does not take into consideration that loss avoidance, compared to the overall expense of implementing a fraud solution, can create ROI value.

Because compliance software does not have a direct and calculable ROI, investment choices are more critical. A solution should be sound, auditable, secure, and effective, with the ability to demonstrate to regulators that the bank's compliance efforts are acceptable and the solution intentionally and substantively supports the user's AML program, which includes customized risk tolerance levels and many other factors unique to the user. Unlike the functionality in many financial service applications, AML automation has responsibility for and can significantly affect intangibles such as reputation, regulator oversight, shareholder confidence, and the ongoing abilities of the financial institution to carry on business activities unhindered by regulator imposed limitations. Regulators now are saying publicly what

they have been saying privately for several years: AML software applications are now affordable and readily available, for institutions of all sizes, and, the automation they provide should be employed to meet AML compliance needs.

		Application Predicts:	
		True (Triggered)	False (Not Triggered)
Actual Outcome	Suspicious	True Positive	False Negative
	Not Suspicious	False Positive	True Negative

Output conditions for analytic decisioning.

In the context of AML, a false positive occurs when software generates an alert saying that a rule, threshold or other condition should be triggered, when in actuality the activity is not suspicious or illicit. A false negative occurs when an actual suspicious activity, an activity for which an alert should have been generated, has been missed. A true positive is when an application generates an alert for an actual suspicious activity, while a true negative is when a system predicts that an event is suspicious or illicit when it is not.

The examination of false positives as a measure of effectiveness has proven problematic because false positive and alert generation rates are often thought of in the same terms as those used in fraud software—that is, how many alerts will the system generate and how many of these alerts are false (not suspicious or illicit)?

Unfortunately, when used as a selection metric in AML software, false positive volume is a disservice to the user, their financial institution, the application, and society. Though money-laundering activities are plentiful, the transactions and related activity making up that volume spread across the globe, are subtle, and are very difficult to find. While fraud will eventually show up in the bottom line, that is not necessarily true of money laundering or terrorist financing. If it is not detected by AML software, it will likely remain undetected. Clearly a different logic must be applied to AML software.

A more accurate measurement of AML technology effectiveness begins with the concept of *optimizing* the application's use. If a bank devotes only 20 "person-hours" a week to investigating alerts, it does no good to have software that generates hundreds of alerts a week regardless of user risk tolerance levels. Therefore, it is suggested that the number of personnel processing alerts *prior* to the installation remain roughly the same afterward because AML technology makes alert investigation easier and more effective. The most significant or riskiest alerts can be raised and evaluated, which in turn better protects the user and society.

Optimization and Multiple Constraints

Many variables contribute to effective implementation and deployment of AML solutions. Due to the complexity of the problem, there can and most often will be more than one "minimum" and "maximum" value for user settings when it comes to alert optimization for AML; in other words, multiple constraints. With AML, the concept of multiple constraints manifests itself in three major contexts.

The first context relates to limits of behavior, such as minimum and maximum acceptable tolerances for whole number counts of events, transaction values or other metrics, and acceptable value ranges. An example would be setting all cash or cash-related transactions to daily limits to avoid the review of all cash transactions. At the ceiling, a \$10,000 daily limit is defined for CTR filing, but a second value should be *optimally* used as a "floor" so that efforts to evade the detection of structuring can be identified. There are many transactions that are not involved in structuring activities, so the goal is to set minimum and maximum limits that allow insignificant cash transactions to be completely ignored while reviewed transactions support the user's risk tolerances. The key is that these values vary over time and between categories. Different risk levels exist for different situations, products, groups, channels, etc., and risk-level tolerances can be

applied with the use of the optimal minimum and maximum settings.

The second context concerns the data analysis used to determine "normal" distributions of data to identify, statistically and holistically, significant relationships, peer groups, etc. The highest and lowest percentages or whole number values of a designated activity are identified with thresholds set to optimize alerts. This incorporates decisioning by the AML software as a risk-based prioritization, not a mere presentation of the most severe or critical alerts.

The third context incorporates absolute mathematical meaning. A particularly apt example of this is linear programming, also known as linear optimization or the problem of maximizing or minimizing a linear function over large amounts of complex or unknown data. This concept, as it relates to AML software, is exemplified by the capability to look at multiple values and/or conditions to determine the suspiciousness of a set of data points. For example, if a transaction volume exceeds a certain amount and the transaction(s) is (are) greater than a determined amount, does the activity warrant a red flag?

The concept of multiple approaches in hybrid software is analogous to the use of different types of math to solve different types of math problems. When faced with a question about angles, geometry is used; for the solving of unknown variables, algebra; for the area under a curve, calculus, and so on. The hybrid solution consists of a variety of tools, techniques, and approaches, optimally combined, to monitor for suspicious activity both in the context of the user's environment and their accepted levels of risk.

The Importance of Effective Software Development

Even the best software evaluation efforts are of no value if the underlying AML program itself is flawed. There are many third-party services available to assess an AML program for effectiveness; this is not the same

as the external audit the law requires. A third-party assessment can help identify gaps in compliance to head off potentially negative events. It can also analyze the environment to recommend action steps for a successful software implementation and optimized installation. A seasoned AML software vendor will offer consulting services that can assess existing policies and procedures. In addition, this individual will analyze implementation needs to support existing and proposed AML program capabilities in terms of risk tolerances, lines of business, market/business requirements and any unique needs. Applying the benefit of this experience can determine whether or not formal statistical data analysis or other efforts should be undertaken to determine the optimal rules, analytics, and settings for their software. When it comes to a successful implementation and the optimization of your AML software, the best alternative is to employ the services of a vendor that has significant experience in deploying hybrid software. With the introduction of literally dozens of AML vendors since the events of 9/11, the vendor review process has become about as complicated as AML detection. Vendors and their solutions must be evaluated on their effectiveness and implementation success.

Deciding which aspects of an AML technology package best meet the needs of an institution is a major concern. A second, but equally important factor is accurately assessing what it will take to deploy a solution successfully. Indeed, the most often cited point of failure regarding AML technology is poor deployment, not product deficiencies.

At a minimum, the following must be considered to ensure effective software deployment:

Utilization of project management expertise that provides:

- The most optimal implementation possible
- Dedicated experts and resources
- A practiced implementation team
- Best practices expertise that minimizes impact to bank resources while maximizing installation resources

Basic services that include:

- A system configuration that incorporates optimal, best practices setup of the software
- Product training for users and system administrators
- Operations procedures defined through business requirements
- Internal and custom interfaces with other applications, as needed
- Support throughout all phases of deployment

Data integration that allows for:

- The most relevant data
- Effective data acquisition
- Data manipulation that allows source system corrections such as reversals and deletions, elimination of duplicates, performance of referential integrity checks, and timely reports
- Data processing that, preferably, leverages existing resources, infrastructure, and processes

Software license and implementation pricing that includes all cost components and which note the following cost categories that are often overlooked:

- Hardware
- Infrastructure/Network requirements

Third-party software costs for maintenance, upgrade, disaster recovery, testing, and eventual replacement

- Financial institution personnel
- Consideration of license alternatives such as ASP/Service Bureau options
- • Clear assessment of vendor relationships, new vendors, existing vendors, proven vendors, etc.

Summarizing Effective AML Technology

In closing, it can be said that the following constituents are critical to the success of AML technology:

- The ability to adapt to changes in regulatory requirements and money laundering typologies.

- Demonstrable best practices capabilities
- An internal audit system capable of storing and retrieving relevant investigation records
- Automatic storage of relevant client and account details with the ability to automate the use of those details to build profiles, on a client's activities
- The ability to compare client behavior/activity to client history, profiles and peer groups.
- Automatic generation and prioritization of alerts
- Automated tracking, reviewing, archiving, and reporting of vast amounts of data
- Active support of the institution's risk program so that it does not have to change to accommodate the technology
- Efficient online user interface that is intuitive and easy to navigate
- Efficient communication conduit between investigator and others outside the process
- Automated workflow that can be customized by the institution to match their process
- Clear demonstration that it meets the expectations of regulators, including archival and query tools that allow quick and easy responses to regulating agencies and other interested parties

The Right Vendor and the Right Technology

Proven vendors with the expertise and financial stability to assure a good product, optimal implementation, ongoing support, and development do exist, despite new technology. They provide solutions written in newer programming languages, plus browser-based technology with a Windows look and feel provide heightened user familiarity and a short learning curve.

Ideally, vendors will also display a facility with a variety of technologies. This allows them to steer clear of functionality gaps, and in turn provide product capabilities that can better support the user's risk-based approach and compliance program. When necessary, the vendor will craft a technology plan to complement

the user's IT and business environment, including the incorporation of AML risk assessment data already collected through the bank's existing processes and systems.

A critical part of Metavante's strategy is its Prime Suite of AML technology products; a hybrid solution designed to meet the AML detection needs at the majority of banks. The BSA Reporter transaction-monitoring module provides a myriad of compliance-related database information and produces the best alert data possible for regulatory compliance. Its components can monitor transactions, account relationships, historical behavior, and peer group comparisons. Seamless access to individual searches and critical information gives you instant results from your Web browser. And that's just a beginning of the protection BSA Reporter provides against financial criminals, terrorists, money launderers, drug traffickers, and other perpetrators with criminal intent.

The Metavante Consulting and Professional Services group is comprised of over 250 resources dedicated to risk management, compliance, revenue improvement, efficiency, sales and service, process redesign, project management, and systems integration. Our Risk Management and Compliance specialists are selected from this group based on a match of their skill set to your risk needs and immediate concerns. We are unique in the industry, as we are seasoned practitioners who leverage banking, process, risk, compliance, and systems knowledge.