Aite PARTNER. ADVISOR. CATALYST.

Global Anti-Money Laundering Vendor Evaluation: A Reinvigorated Market

MAY 2011

Julie Conroy McNelley

This document is an excerpt of an independent researchreport published by Aite Group in May 2011.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

IMPACT POINTS

- To gauge the current state of anti-money laundering market, Aite Group interviewed 36 financial institutions spanning five continents and ranging in size from US$800 million in assets to more than US$1 trillion in assets, as well as 18 leading vendors in the global anti-money laundering space between January and April 2011.
- In the United States alone, regulatory actions against financial institutions for AML violations over the last year have resulted in fines and settlements exceeding US$800 million. With the convergence of increasing regulatory scrutiny, new regulation, and increasing payments volumes and message types, this number will continue to grow.
- Between 2009 and 2010, more than 1,200 new AML installations were implemented by vendors interviewed.
- As a result of the converging growth drivers, the global anti-money laundering transaction monitoring software market is growing at a healthy pace, and will continue to do so for the next few years. The global market is currently at US$450 million, and will grow at a compound annual growth rate (CAGR) of 9% over the next few years, reaching US$690 million in 2015. Market drivers include rapid growth in the Asia-Pacific, the Middle East, and Africa; financial institutions in the United States and Europe replacing outdated solutions; and smaller financial institutions replacing manual processes with automated solutions.
- Key components of AML solutions include customer due diligence (CDD), suspicious activity monitoring (SAM), case management, and watch-list filtering. The solutions in the marketplace fulfill these needs to varying degrees. Some vendors offer complete end-to-end solutions, while others target one part of the problem. Increasingly, vendors are also positioning themselves as one-stop-shop enterprise risk management (ERM) solutions serving both AML and fraud prevention needs.
- Financial institutions should have a solid understanding of how their needs match up with vendor competencies. Based on information provided by vendors through RFI responses, phone interviews, product demos, feedback provided by client references, and Aite Group's own knowledge of the industry, Aite Group provides analysis of key strengths and weakness of each of the vendors, and recommends vendors for financial institutions of various sizes.

INTRODUCTION

Anti-money laundering (AML) technologies have been enjoying a fresh wave of demand across the globe during the last few years, driven by the convergence of increasing regulation, high-profile regulatory enforcement actions, and next-generation technologies that can address both AML and fraud management needs across the enterprise. To evaluate the marketplace, Aite Group interviewed 18 global AML compliance vendors and 36 financial institutions between January and April 2011.

Long viewed as a mature market in the United States, recent enforcement actions have had the effect of creating a flurry of re-evaluation of current solutions and investment in new AML technology. At the same time, new global markets are emerging—countries around the world have taken steps over the last decade to implement, reinforce, and in some cases, just plain enforce, their own AML regulatory approach. This report begins with an overview of the regulatory environment, proceeds with an overview of the critical components for AML solutions, and concludes with analysis of the leading vendors in the space.

REGULATORY DRIVERS

The legislative framework for AML dates back to 1970 with the U.S. enactment of the Bank Secrecy Act (BSA), which required financial institutions to track cash transactions and file reports detailing any suspicious activity. In 1986, the U.S. Money Laundering Control Act criminalized the act of money laundering. Then, in 1989, the Financial Action Task Force (FATF) was formed at a G7 Summit as an intergovernmental body to develop international standards for AML regulation. Between 1991 and 2005, three separate EU money-laundering directives were issued, codifying into EU law additional anti-money laundering regulation based on the FATF model.

With the enactment of the USA Patriot Act in 2001, the purview of money laundering regulation was significantly expanded to encompass terrorist financing. In the years since 2001, a number of countries have used the USA Patriot Act as a model for their own anti-money laundering regulation, particularly in the Middle East and Africa, which previously did not have much in the way of anti-money laundering regulation.

Table A: Legislative Framework for AML

Year	Jurisdiction	Effort	Description
1970	U.S.	Bank Secrecy Act	Requires FIs to track cash transactions, file CTRs for transactions of US$10,000 or greater, and report suspicious activity
1986	U.S.	Money Laundering Control Act	This act criminalized the act of money laundering, prohibited structuring to avoid CTR filings, and introduced criminal and civil forfeiture for BSA violations
1989	Global	FATF	An intergovernmental body established by the G-7 to develop policies to combat money laundering and terrorism funding
2001	U.S.	USA Patriot Act	This piece of legislation significantly upped the ante and the regulatory burden on U.S. institutions, and has served as a

Year	Jurisdiction	Effort	Description
			driver of AML regulation in other countries
2005	EU	EU Third Money Laundering Directive	The three EU anti-money laundering directives enacted between 1991 and 2005 are based on the FATF model

Source: Aite Group

ENFORCEMENT ACTIONS DRIVING ADOPTION

While new legislation has driven the AML technology market in the Asia-Pacific, the Middle East, and Africa, enforcement actions are causing many financial institutions (FIs) in the North American and European markets to take a fresh look at their approach. Table B provides an overview of major enforcement actions taken by the U.S. government over the last couple of years. The enforcement agencies behind these actions include the Financial Crimes Enforcement Network (FinCen), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), the Department of Justice (DOJ), the Manhattan District Attorney's office, and the Office of Foreign Asset Control (OFAC). These actions have spurred a number of financial institutions to reevaluate the effectiveness of their AML program and look for gaps in control and oversight.

Table B: Recent U.S. AML Enforcement Actions

Date	Institution name	Agency(ies)	Amount	% of total assets	Violations
March 2011	Pacific National Bank	FinCen, OCC	US$7 million	1.9%	Failure to implement an effective AML program
February 2011	Zions First National Bank	FinCen, OCC	US$8 million	.016%	Failure to accurately monitor and report remote deposit capture and wire activity specific to foreign correspondent business
August 2010	Barclays PLC	DOJ, Manhattan DA	US$298 million	.015%	Facilitated and concealed wire transfers to and from blacklisted countries
May 2010	Royal Bank of Scotland	DOJ	US$500 million	.014%	Facilitated and concealed wire transfers to and from blacklisted countries
March 2010	Pamrapo Savings Bank	FinCen, OTS, DOJ	US$6 million	1.1%	Failure to implement an effective AML program
March 2010	Wachovia Bank	FinCen, OCC, DOJ	US$160 million	.02%	Failure to accurately monitor and report RDC and wire activity specific to foreign correspondent business; failure to conduct adequate customer due diligence
December	Credit	DOJ,	US$536	.05%	Facilitated and concealed wire transfers

Date	Institution name	Agency(ies)	Amount	% of total assets	Violations
2009	Suisse	Manhattan DA, OFAC	million		to and from blacklisted countries
April 2009	Doha Bank	FinCen, OCC	US$5 million	.10%	Failure to monitor and report activity related to funds transfers, pouch activity, demand draft services, and correspondent relationships
January 2009	Lloyds TSB	DOJ	US$350 million	N/A	Facilitated and concealed wire transfers from blacklisted countries

Source: FinCEN, Aite Group

Many of the largest fines were the result of electronic funds transfer activities by large global financial institutions in which transfers to banned countries such as Iran and Sudan were being facilitated and actively concealed by the bank. This was the result of a lax command and control structure that allowed local offices to engage in illegal activity undetected. In the case of ABN AMRO, which was subsequently acquired by the Royal Bank of Scotland, it was established that the bank went so far as to establish a special manual queue to flag payments involving sanctioned countries so that the bank could eliminate any suspicious text. It even added instructions to payment manuals on how to process transactions with sanctioned countries in order to circumvent AML regulations.

As a result, many FIs are re-examining their controls to ensure appropriate checks and balances are in place to prevent rogue behavior by local offices. Where local data privacy laws permit, this includes centralizing AML screening and operational activity in one physical location. Many legacy or homegrown AML solutions are not sophisticated enough to facilitate this on their own, and a number of institutions are turning to new solutions to help with these initiatives.

Another major driver of enforcement actions has been the failure of smaller financial institutions to implement effective AML programs. Historically, these institutions often had little or no technological process in place. While these fines are much smaller in absolute dollar volume, for the institutions in question they are quite significant as a percentage of total asset size, and have caused a number of small FIs to reexamine their current approach to AML compliance.

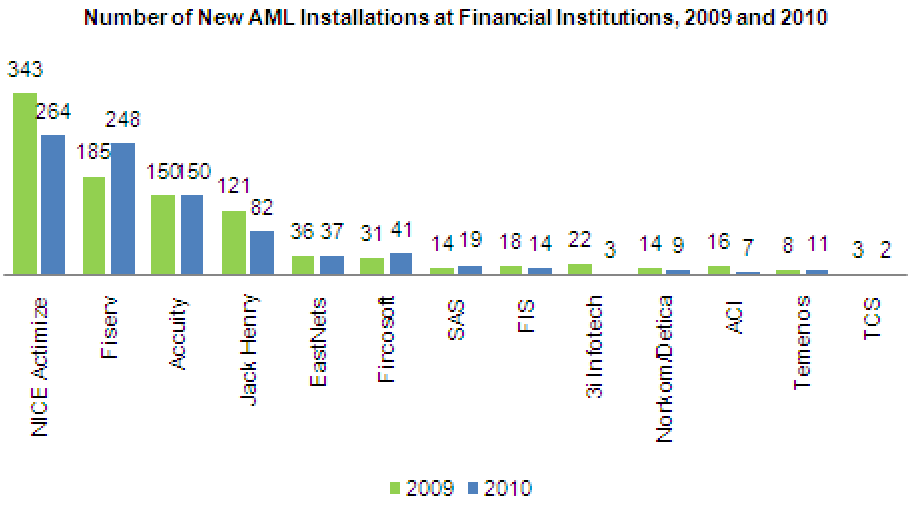
GEOPOLITICAL ENVIRONMENT

The geopolitical environment also can have a significant impact on the day-to-day volume of transactions that AML systems must screen, as well as influence the focus of regulatory scrutiny. The "Arab Spring," a series of revolutionary movements that spread across a number of Middle Eastern countries in early 2011, provides a perfect example of this. Due to a resolution passed by the United Nations Security Council on February 25, 2011, FIs are obligated to identify and stop transactions relating to Libyan leader Muammar Gaddafi. The regulatory mandate also obligates FIs to identify transactions associated with any business in which Gaddafi or his family members hold any beneficial ownership. This is a complex problem, which requires a sophisticated level of analytics to attack. The exceptions resulting from AML screening can vary widely based on geopolitical events. While it not possible to anticipate these events when budgeting for headcount, highly flexible and analytic systems can help minimize the impact to FIs.

AML SPEND TREND

To meet the increasing volume and complexity of AML activity, more than 1,200 new AML installations were implemented in 2009 and 2010 by vendors interviewed (Figure 1), with NICE Actimize leading the way in terms of volume of new installations, which were direct comprised of direct installs and via hosted solutions at channel partners such as Pershing. Fiserv also enjoyed rapid growth fueled by integration of the NetEconomy solution with Fiserv's core banking systems.

Figure 1: Number of New AML Installations 2009 and 2010



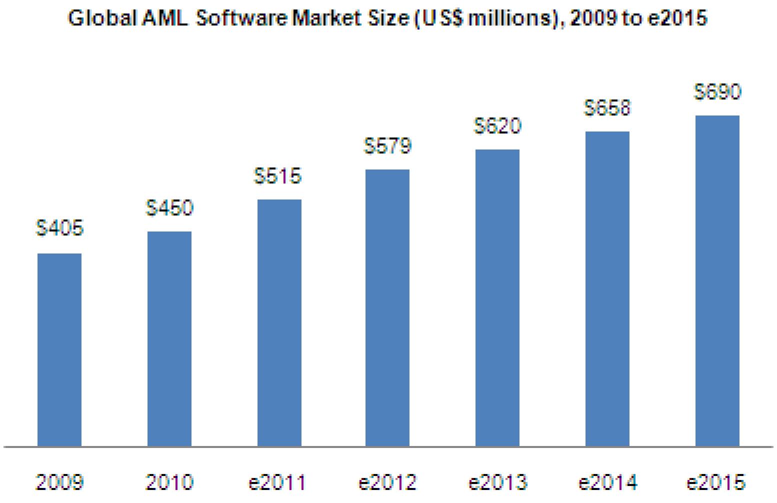
Source: Aite Group, vendor data

Pricing for AML software solutions typically consists of an annual license fee as well as an annual maintenance fee. Annual license fees are usually based on an institution's asset size, transaction volume, number of customer accounts, number of business lines using the solution, or a combination of these factors. If deployed as a part of an enterprise risk management solution, in which modular units are deployed for both fraud prevention and risk management, unique license fees tend to apply to each module, depending on the volume processed through each. Economies of scale are reaped through sharing the cost of implementation across multiple business units or cost centers. The annual maintenance fee can run anywhere from 15% to 30% of the annual licensing fee. Some vendors allow customers to elect the support levels they wish to have (24/7 versus support limited to business hours only), and tailor the annual maintenance fee accordingly. AML license fees can range from US$40,000 for a small credit union or community bank using a hosted solution to US$1.5 million for a large FI using on-site software.

As a result of the converging growth drivers, the global AML transaction-monitoring software market is growing at a healthy pace and will continue to do so for the next few years. The global AML software market has reached US$450 million, and will grow at a CAGR of 9%, reaching

US$690 million in 2015, as depicted in Figure 2. Market drivers include areas of rapid growth such as the Asia-Pacific, the Middle East, and Africa; FIs replacing outdated solutions; and smaller financial institutions replacing manual processes with automated solutions.

Figure 2: Global AML Software Market Size



Source: Aite Group

KEY ELEMENTS OF AML SOLUTIONS

Key components of AML solutions include customer due diligence (CDD), suspicious activity monitoring, case management, and watch-list filtering. The solutions in the marketplace fulfill these needs to varying degrees. Some vendors offer complete end-to-end solutions, while others focus solely on targeting one part of the problem. Increasingly, vendors are also positioning themselves as one-stop-shop ERM solutions for both AML and fraud prevention. The following sections describe the key elements of AML compliance solutions. Vendors offering all of these components typically sell them in modular fashion; FIs can choose to implement one or multiple modules depending on their needs.

CUSTOMER DUE DILIGENCE

Customer due diligence, also known as Know Your Customer, is the process by which a bank verifies the identity of the individual or entity with which it is doing business. This is then supplemented by ongoing due diligence (ODD), which consists of analytic routines that verify that the information provided by the customer is consistent with the subsequent transaction patterns and behaviors associated with the customer. Key criteria that FIs should look for in a CDD solution includes the following:

- Risk ratings that can be used to prioritize manual investigations
- The ability to incorporate external database calls for verifying the identifying information provided by the customer
- For FIs with a global presence, the ability to support different data elements required by different jurisdictions

SUSPICIOUS ACTIVITY MONITORING

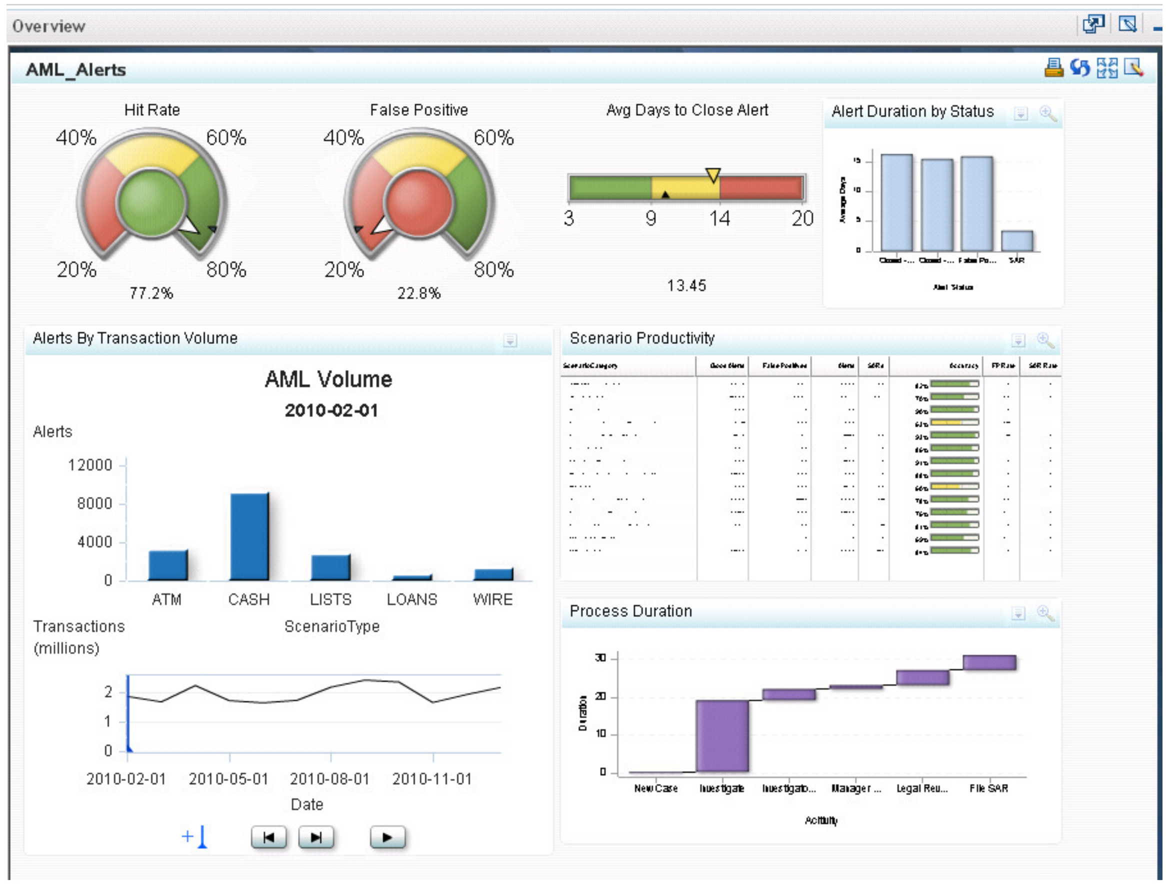
AML solutions are designed to detect the common flows of money laundering, which typically proceed as follows:

- **Placement:** Placing funds generated from illegal activity into circulation. This often involves structuring, a series of small transactions to avoid triggering the reporting requirement that is in place for transactions US$10,000 and greater.
- **Layering:** The origin and funds trails are obfuscated through a series of transactions between accounts at multiple institutions.
- **Integration:** The funds are re-introduced into the economy, often disguised as normal business earnings.

Best-in-class transaction monitoring solutions use a combination of analytics and rule sets to detect suspicious activity. While rule sets are useful in looking for known suspicious behavior patterns, it is impossible to create a rule set for every potential scenario, and analytics are required to detect unknown scenarios that are indicative of money laundering. AML analytics typically provide the ability to create alerts if a user's behavior deviates from peer behavior, historical behavior patterns, or expected behavior patterns.

Ongoing tuning is an important part of maintaining AML compliance, and is a key item that regulators look for when conducting audits. Many of the vendors interviewed provide interfaces for business users to perform the tuning on an ongoing basis so that IT personnel do not have to be involved. These interfaces include plain, non-technical language; drop-down boxes; and drag-and-drop widgets that allow authorized users to easily build new rules. Some provide sandbox environments so that business users can test their new rule sets prior to deploying them and gauge whether the new rule will have unintended consequences (e.g., an overwhelming amount of alerts that makes it impossible to prioritize the truly high-risk investigations).

Figure 3: Sample AML Dashboard



Source: SAS Institute

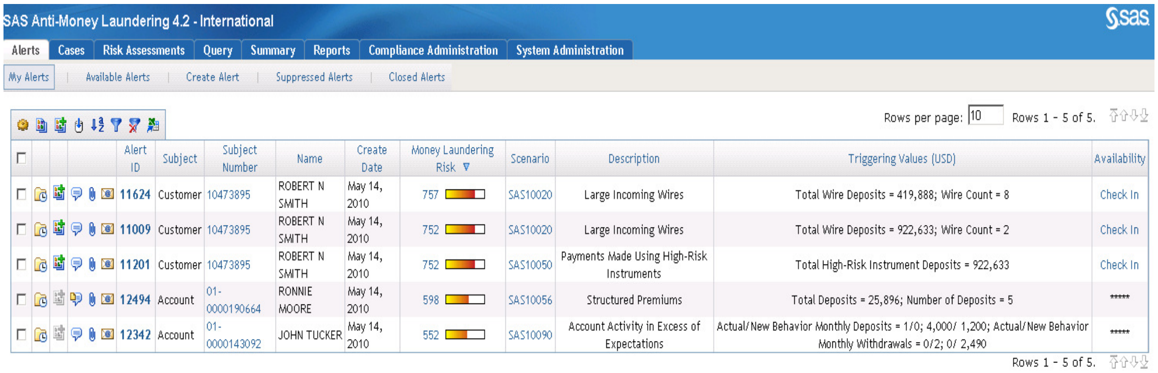
INVESTIGATION

The investigation layer of AML solutions typically consist of alert management, case management, link analysis, and automated reporting.

ALERT MANAGEMENT

Alert management tools assist with routing alerts to the appropriate investigator. They can facilitate workflow prioritization, and many solutions provide the option for users to receive automated notification via email or SMS when new alerts enter the system. SAS has a feature-rich alert management system that provides a great example, as displayed in Figure 4.

Figure 4: Sample Alert Management Interface



□	Alert ID	Subject	Subject Number	Name	Create Date	Money Laundering Risk ▼	Scenario	Description	Triggering Values (USD)	Availability
□	11624	Customer	10473895	ROBERT N SMITH	May 14, 2010	757	SAS10020	Large Incoming Wires	Total Wire Deposits = 419,888; Wire Count = 8	Check In
□	11009	Customer	10473895	ROBERT N SMITH	May 14, 2010	752	SAS10020	Large Incoming Wires	Total Wire Deposits = 922,633; Wire Count = 2	Check In
□	11201	Customer	10473895	ROBERT N SMITH	May 14, 2010	752	SAS10050	Payments Made Using High-Risk Instruments	Total High-Risk Instrument Deposits = 922,633	Check In
□	12494	Account	01-0000190664	RONNIE MOORE	May 14, 2010	598	SAS10056	Structured Premiums	Total Deposits = 25,896; Number of Deposits = 5	*****
□	12342	Account	01-0000143092	JOHN TUCKER	May 14, 2010	552	SAS10090	Account Activity in Excess of Expectations	Actual/New Behavior Monthly Deposits = 1/0; 4,000/ 1,200; Actual/New Behavior Monthly Withdrawals = 0/2; 0/ 2,490	*****

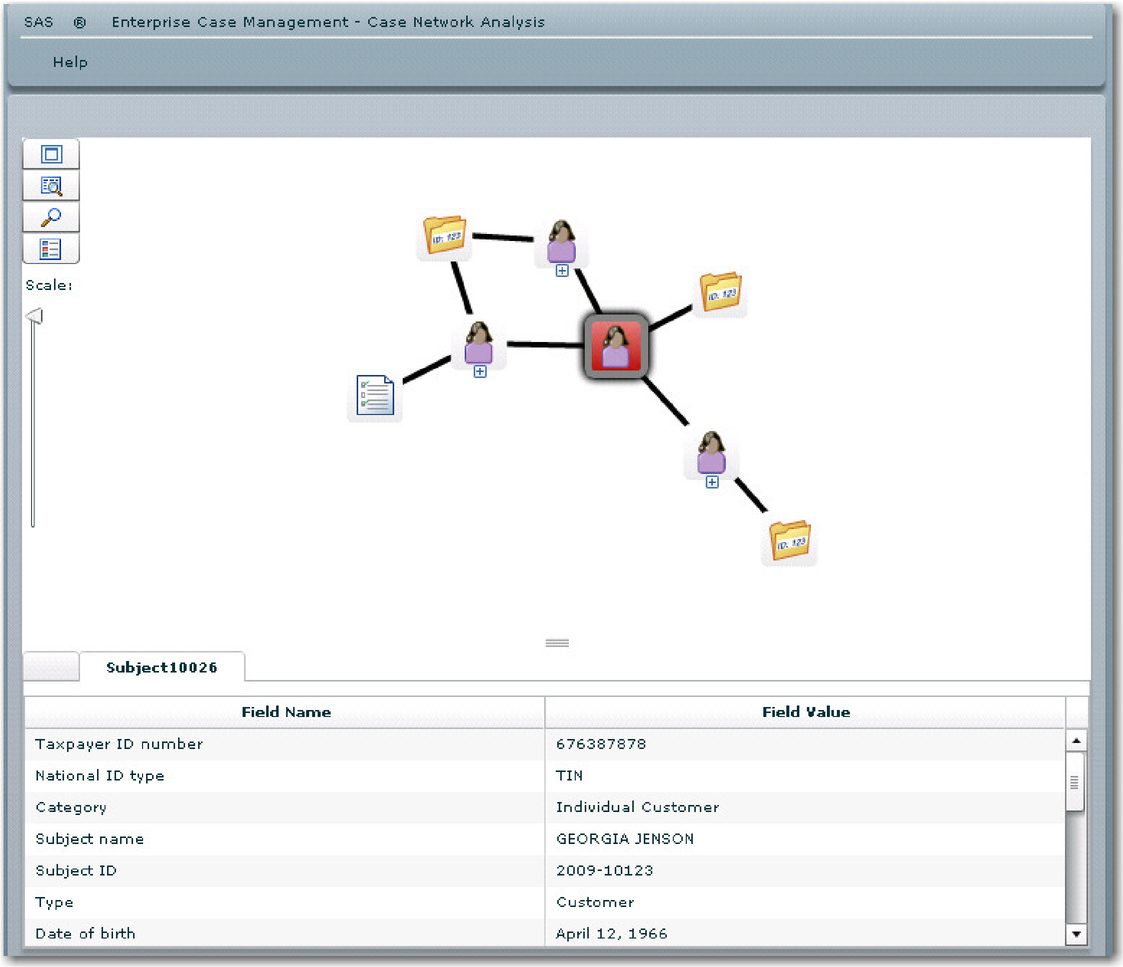
Rows 1 - 5 of 5.

Source: SAS Institute

CASE MANAGEMENT

Case management tools provide the aggregation of all data, notes, and activities relating to an investigation in a central location. This not only aids in the investigation process, but also serves as a system of record for compliance purposes and as a central data repository to aid law-enforcement investigations. Case management tools also help manage workflow and assist in appropriate classification of suspicious activity. A good example of a case management interface is displayed in Figure 5.

Figure 5: Sample Case Management Interface



Field Name	Field Value
Taxpayer ID number	676387878
National ID type	TIN
Category	Individual Customer
Subject name	GEORGIA JENSON
Subject ID	2009-10123
Type	Customer
Date of birth	April 12, 1966

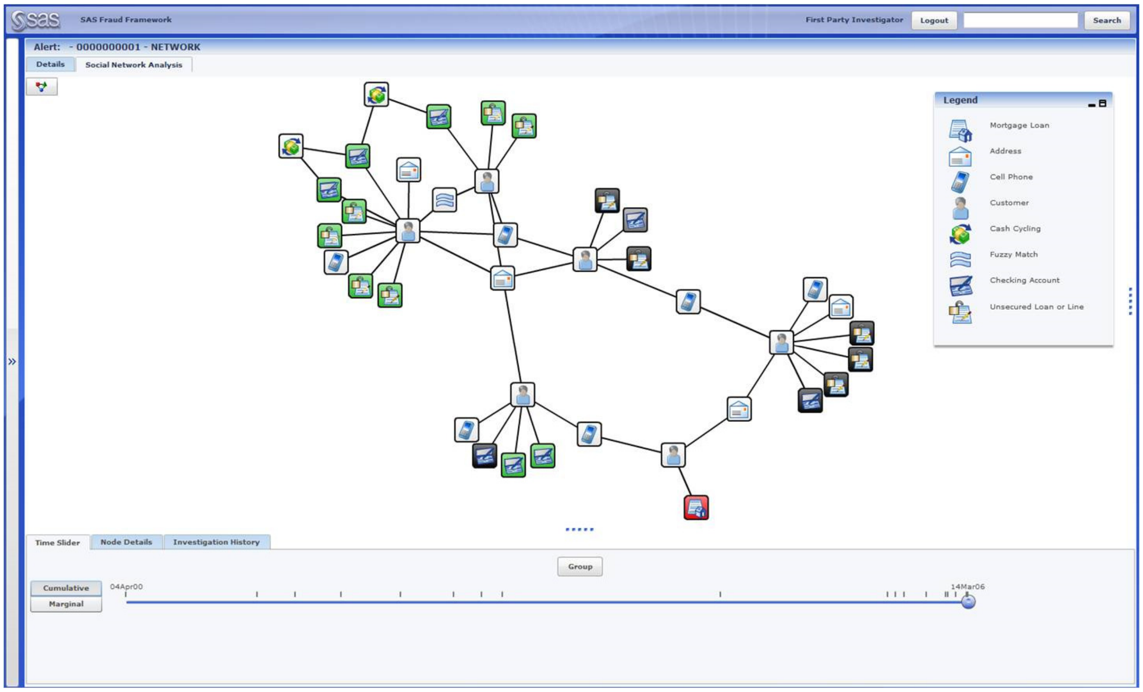
Source: SAS Institute

Best-in-class AML case management tools also provide the ability to automate reporting into local jurisdictions' governmental financial investigations unit, for example, automated Suspicious Activity Report (SAR) submissions to FinCen in the United States.

LINK ANALYSIS

Link analysis tools sift through the data repositories at financial institutions and discover connections between customers and accounts. Some connections are innocuous, others highly suspicious. Effective link analysis tools can differentiate between these, prioritizing the suspicious networks and providing users with a visualization tool that helps them understand and investigate the linkages. While link analysis can also be homegrown with database tools, more sophisticated link analysis solutions help minimize the false positives that are natural products of multiple people sharing the same household, and can help hone in on truly anomalous networks.

Figure 6: Sample Link Analysis Visualization



Source: SAS Institute

There is was a wide variance in the reported effectiveness of link analysis tools among the financial institutions that Aite Group interviewed. Due to the nature of link analysis, high levels of false positives can dilute the effectiveness. The best results were reported when FIs had a wide variety of tools at their disposal to control these false positives. Maturity of the link analysis solution also plays a big part in effectiveness.

WATCH-LIST FILTERING

Financial institutions are obligated to screen customers and transactions against numerous watch lists. These include sanctions lists of entities with which financial institutions are prohibited from transacting, as well as the Politically Exposed Persons (PEP) list of individuals who hold a position of prominence in a foreign government or foreign-owned corporation. Financial institutions are not prohibited from transacting with PEPs, but certain members of this group represent a higher risk, and enhanced due diligence procedures are required under anti-money laundering regulations. There are nearly 1,000,000 names on the global PEP list, and nearly 120 sanctions lists that collectively have more than 20,000 profiles. One of the biggest challenges to watch list screening is creating an effective screening process that minimizes false positives and false negatives.

The false positive problem is further complicated by the fact that there are multiple spellings for many names, particularly names that are transferred from character-based languages to the Western alphabet. There are a number of fuzzy- and phonetic-matching protocols that vendors apply to assist in the approach. A key element that is important in helping to create the appropriate balance between false positives and false negatives is the context for the match; the AML solution should be able to help evaluate the context for the match so that a Charles Taylor on the OFAC list does not create a false-positive match for every individual that lives on Charles Taylor Street in Queensland. In addition, the ability to be able to process and evaluate unstructured data, such as the invoice accompanying a trade finance transaction, can be critical in helping determine whether a transaction is innocuous or merits additional scrutiny.

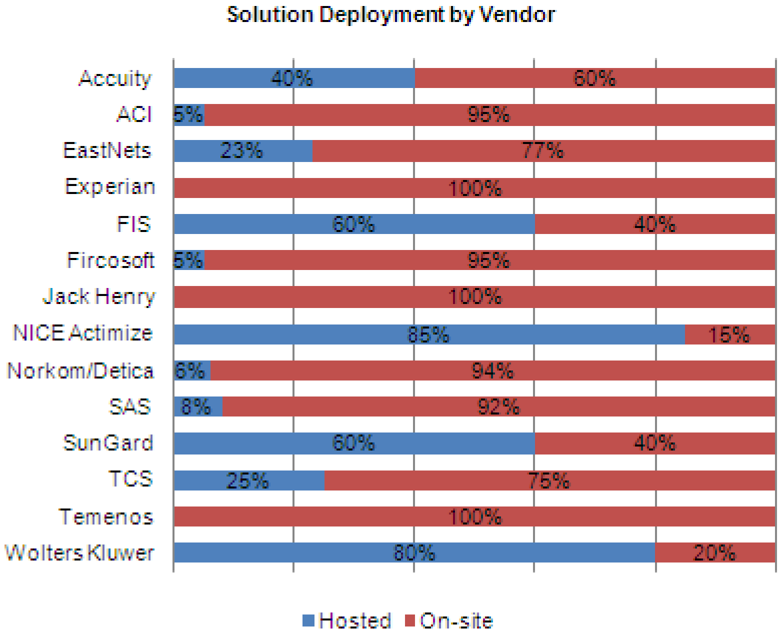
FRAUD PREVENTION

Many vendors position their solutions as enterprise risk management platforms, which can address both the fraud management and AML needs of a financial institution through a single platform implementation. These solutions have the ability to deploy different rule sets depending upon the use case, and the case management layer can be segregated or aggregated depending on user-level permissions. FIs can deploy one technology platform that can address multiple needs across the institution. These solutions can also help facilitate the sharing of data between the AML and fraud-prevention sides of the business in recognition of the fact that fraud and AML incidents are increasingly interwoven.

DEPLOYMENT OPTIONS

Due to the sheer volume of data that needs to be processed, large financial institutions tend to license AML software for on-site deployment. Many large FIs are increasingly choosing to deploy this in a hub-and-spoke model, where a central office hosts the processing (to the extent local law allows), and local offices work the alerts with oversight from the central office. This helps address the command and control issues that resulted in heavy enforcement actions cited in Table B. Smaller financial institutions, on the other hand, have more deployment flexibility; many choose to leverage hosted solutions, which can substantially reduce the implementation time and total cost of ownership, particularly if those solutions are hosted by the FI's core banking system vendor. Figure 7 shows a breakdown of deployment environment by vendor for vendors willing to share this data publicly.

Figure 7: Vendor Deployment Breakdown



Source: Aite Group

VENDOR PROFILES

Vendor	Comprehensive solution	Depth of experience	Customer support	Performance	Total
SAS	5	5	4	4	18
NICE Actimize	5	5	4.3	3.4	17.7
Norkom/Detica	5	5	3.3	3.8	17.1
3i-Infotech	4	4	4.25	4	16.25
Fiserv[1]	5	5	2.75	3.5	16.25
ACI Worldwide	3	4	3	4	14
TCS	4	3	3	3	13

Source: Aite Group

The information in this section is based on information provided by vendors through RFI responses, phone interviews, product demos, feedback provided by client references, and Aite Group's own knowledge of the industry.

SAS

SAS, headquartered in Cary, North Carolina, is the world's largest privately held software company, specializing in business analytics. One of the market leaders in the AML market, SAS' solutions are in use by some of the largest financial institutions in the world, including Bank of America, Bank of Tokyo, and Commonwealth Bank of Australia. FinCen leverages SAS' link analysis capability to search for linkages across all of the SARs it receives from financial institutions. SAS also targets smaller financial institutions, with a credit union and regional banks among the 113 FIs using its AML solution.

PLANNED ENHANCEMENTS

SAS AML 5.1 will be released in the third quarter of 2011. The biggest enhancement will be the inclusion of a consortium predictive model that increases the quality of work items so that institutions can focus resources on high-risk entities while significantly reducing false positives. Other enhancements include the following:

- Packaged data management routines to reduce the effort of migration
- Enhanced network visualization to display payment relationships
- Dow Jones watch list support
- Enhanced regulatory reporting console

[1] The ratings resulting from Fiserv customer interviews were segregated by global and U.S. installations, in recognition of the vastly different implementation and customer experience between the two.

Ratings for both performance and responsiveness with customer service requests were 4 on a scale of 1 to 5, with 5 meaning “very satisfied”. Strengths cited included the wide range of prepackaged scenarios that were available with the solution, all of which are easy for FIs to adjust as needed. When asked about areas for improvement, the comprehensiveness of user training was cited, as well as the fact that the implementation was more difficult than anticipated; the perception was that expectations around the amount of work involved were not appropriately set.

SAS’ architecture is a plus for smaller FIs that don’t have a data warehouse in place, as it provides the data schema for creating a data mart, and can support a number of different relational databases. SAS also provides a Teradata solution for large FIs that can process a vast amount of data in a relatively short period of time. In a proof of concept with one large FI client, SAS demonstrated an ability to process 2.5 billion transactions well within the allotted processing window. SAS also brings a significant amount of analytic firepower to the space, given its roots in statistical solutions.

Table C: SAS Key Strengths and Areas for Improvement

Strengths	Areas for improvement
Prepackaged scenarios	Training
Analytics	Ease of implementation
Data integration studio	
Scalability	

Source: Aite Group

CONCLUSION

Coupled with a rising compliance bar, ever-increasing quantities of legislation have reinvigorated the AML technology market. Here is a series of recommendations for financial institutions:

- Financial institutions should evaluate their current AML compliance mechanisms to determine whether they have progressed with the changing times—regulators are certainly doing so during examinations.
- Smaller financial institutions should look for a solution that can be managed with limited resources, yet which provides the comprehensive, risk-based compliance required in today's rigorous regulatory compliance environment.
- All financial institutions should ensure that their vendor solution can offer a comprehensive collection of rule sets to cover the AML typologies and scenarios for which regulators will be looking, and that those rule sets are easy to tailor for each country in which the FI has a presence.
- Financial institutions in the market for a new solution should ask prospective vendors what level of revenue is reinvested in R&D on an annual basis, a key determinant of whether the solution will remain viable as a long-term investment. These figures varied widely among the vendors in this report, from 3% to 45%, with a mean of 18%.
- Key elements to look for in watch-list filtering solutions include the ability to apply different rule sets to new customer screening and payment transaction screening; provide four-eye review; learn from false positives and reduce their impact going forward; use unstructured data in the detection process; and detect nuanced data sets such as Bank Identification Codes that represent liquidity risk. The latter is not a common occurrence, but proactive detection of the outlier cases can save FIs tens of millions of dollars.
- Financial institutions should ask their vendor whether they provide a sandbox where rule changes can be tested prior to rolling out in production to help gauge unintended consequences (in the form of reams of accidental reports).
- FIs with more specialized applications, like trade finance, should determine how the peer group profiling works to ensure that the logic meets the needs of the bank.
- Analytics will increasingly come into play as AML exception volumes increase and the lines between AML and fraud blur. Rule sets are a good start, but rules can only identify a finite number of scenarios. Analytics are required to look beyond the individual rules to find broader patterns.
- Data sharing across financial institutions could be the next frontier of AML. This is a nascent concept, but a few experiments are taking place on this front. If successful, these experiments could raise the bar for all financial institutions.

RELATED AITE GROUP RESEARCH

Global Bank Technology Trends 2011, May 2011.

Enterprise Fraud Management: Investments in Integration, February 2011.

Chasing Compliance: Things That Go Bump in the Night, November 2009.

Trends in Anti-Money Laundering Compliance: Evolving Practices and Strategies, August 2008.

Resources for Anti-Money Laundering Compliance: Retail Banks on Technology and Staffing Trends, July 2008.

ABOUT AITE GROUP

Aite Group is an independent research and advisory firm focused on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, securities & investments, and insurance, Aite Group's analysts deliver comprehensive, actionable advice to key market participants in financial services. Headquartered in Boston with a presence in Chicago, New York, San Francisco, London, and Milan, Aite Group works with its clients as a partner, advisor, and catalyst, challenging their basic assumptions and ensuring they remain at the forefront of industry trends.

AUTHOR INFORMATION

Julie Conroy McNelley

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Patrick Kilhaney
+1.718.522.2524
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com