



DYNAMIC, RISK-BASED ASSESSMENT OF CUSTOMERS AND TRANSACTIONS

Identifying, investigating and reporting suspicious patterns of behavior with
SAS® Anti-Money Laundering



Table of Contents

Executive summary	1
A dynamic, risk-based AML system	2
What would you gain with a more effective AML program?	2
Monitor risks across the institution.....	2
Allocate resources to the most meaningful cases	3
Demonstrate knowledge of high-risk accounts and their activity	3
Adapt to changing risks.....	4
Toward a new model of detection and prevention	4
SAS® Anti-Money Laundering	5
Identify and rank suspicious activity for investigation, without wasting time and energy on trivial alerts or false positives	6
1. Matches with known money-laundering schemes.....	6
2. Matches with internal or external name lists.....	7
3. Occurrence of high-risk transactional behaviors.....	7
4. Match to high-risk KYC/CIP profiles.....	7
5. Suspicious flows of money among accounts.	8
7. Reported suspicious activity.	9
Investigate potentially suspicious accounts or activity	11
Meet regulatory reporting requirements with automated generation of SARs/STRs and supporting documentation	12
Monitor and manage system access and utilization	12
Summary	13
About SAS	14

Executive summary

The events of 9/11 and subsequent terrorist attacks have increased regulatory emphasis on anti-money laundering (AML) in order to stem the flow of illicit financial activity. Many institutions initially made modest technology investments in order to meet minimum AML requirements. However, this minimalist approach can't provide an enterprisewide view of money laundering risk and it actually increases an institution's total cost of ownership due to inefficient investigations, higher staffing costs, the need for successive technology investments, and little value being contributed to other functions, such as marketing and loss recovery management.

Today, financial institutions are finding it necessary to strengthen their AML programs in order to effectively identify and report suspicious activity, meet new regulatory mandates and strategically manage compliance risk. For enterprises with moderate- to high-risk exposures, this calls for a rigorous automated system, such as SAS Anti-Money Laundering.

SAS Anti-Money Laundering not only detects the subtle behavior patterns that could signal criminal activity, but also provides powerful tools for conducting investigations, reporting suspicious activity and providing the reports needed by examiners, auditors and management. The solution can be installed directly or hosted by an application service provider.

A risk-based monitoring and investigation system is a vital component of an effective and compliant AML program, and financial institutions now have a proven way to detect and track suspicious patterns of behavior relative to their unique risks, instead of just one-size-fits-all rules and account name lookups. With SAS, institutions can capture and organize all customer activity, monitor that activity against industry-specific indicators of criminal behavior, investigate and document suspicious cases, and produce required regulatory reports—all within an integrated solution built on SAS' award-winning data management and analytic capabilities.

In response to requests from global financial institution customers, SAS released a new version of SAS Anti-Money Laundering that added new features to enhance the ability to identify suspect relationships and high-risk accounts and to investigate those findings in an appropriate and timely way, including:

- Advanced analytics to detect unknown patterns of behavior, visually display the flow of funds among accounts and uncover variances against normal behavior and expected activity.
- Greater transparency into customer transactions, so it's easier to see closed or suppressed cases in support of audit and regulatory review processes.
- Visual indicators and background attachments that enable investigators to quickly see if a case has been worked or requires urgent attention.

Regulatory scrutiny and fines are on the rise. Money launderers are more resourceful than ever. Now is the time to protect your institution's reputation and compliance status.

- Strategically manage compliance risk.
- Meet stringent government regulations.
- Protect shareholder confidence
- Maintain a strong reputation.

A dynamic, risk-based AML system

Criminals and terrorists have been resourceful and persistent with their money-laundering activities—accounting for an estimated \$500 billion to \$1.5 trillion a year, globally. Although most laundered money stems from drug trafficking and organized crime, the events of September 11, 2001, put the spotlight on funding terrorist activities.

The USA PATRIOT Act, signed into law the following month, expanded the requirements for detecting and reporting suspicious activities that could indicate money laundering or terrorist financing. So did equivalent AML regulations around the world, such as the European Union's Third Money Laundering Directive. Targeted for implementation by January 2007, the "Third Directive" creates a uniform regime of compliance that expands the definition of "client due diligence," broadens requirements for client/account monitoring, and raises the expectation for banks to adopt risk-based management approaches.

In recent years, headlines have focused on high-profile enforcement actions—some exceeding \$80 million in fines. However, the more pressing, day-to-day concern for financial institutions is simply the cost of compliance. In an effort to meet basic requirements at minimal cost, many firms have chosen AML systems based on low entry price. Unfortunately, a minimalist strategy can actually be quite costly over the long term, for several reasons:

- The Know Your Customer/Customer Identification Program (KYC/CIP) system is probably not integrated with a transaction monitoring system.
- There's little information about a specific event or party, which leads to longer and more error-prone investigations.
- There's little or no insight into customers or behaviors where the compliance costs unnecessarily exceed the risks.

Finally, this short-sighted approach cannot support an enterprise-wide strategy to manage the reputation, operational, legal and concentration risks associated with money laundering.

What would you gain with a more effective AML program?

An effective AML compliance program must address the following management imperatives.

Monitor risks across the institution

Financial institutions have vast repositories of information about customers, their transactions and external databases. Trouble is, much of that data isn't integrated into AML programs. With typical AML systems, compliance analysts are doing well to just detect basic trends and simple matches against known illegal activities.

Few organizations can correlate potentially suspicious behaviors across disjointed systems and a multitude of risk factors. Most automated AML systems only look at transactions and do not take advantage of broader institutional knowledge, such as Customer Information Program (CIP) data, prior high-risk events, risk lists and previous investigations—either for identifying or investigating potentially illegal activities.

Allocate resources to the most meaningful cases

Many AML systems apply the same, limited set of if/then rules to identify suspicious transactions. With time, compliance officers and regulators often discover these rules are overly broad or not specific to the institution's real money laundering risks. These institution-specific risks are easy to overlook, leaving the institution exposed to greater regulatory scrutiny and putting compliance staff under greater pressure. Just as troubling, the rules-based system can trigger too many false positives and overwhelm compliance staff with busy work. At the very least, the increased volume of work items may diminish the credibility and energy of AML monitoring staff and distract front-line staff from their primary responsibilities.

Financial institutions need a way to:

- Adjust scenarios and risk factors to minimize the incidence of false positives.
- Focus on cases that are significant, rather than chasing all simple alerts.
- Differentiate acceptable compliance risk from unprofitable compliance legwork.
- Identify the highest priority cases to be investigated, and in what order.

Demonstrate knowledge of high-risk accounts and their activity

AML monitoring staff need to justify their review actions to regulators. But what if the AML system simply flags incidents as high-risk, yet doesn't say why? If regulators don't have faith in the consistency and accountability of investigative procedures, they will question your processes more closely.

Yet many AML systems do not present a comprehensive view of customer activity, much less customer risk. Investigators may have trouble tracking activities that led to the alert. Case history can be fragmented, especially if a case passes through several investigators' hands, and SARs/STRs often must be produced manually. If regulatory reports are filed outside the monitoring system, it's difficult to use this information for improved analysis.

The ideal AML solution explains why an event or entity represents a high risk to the institution, and it displays enough information to the investigator to support a clear decision process. Further, risk scores are windows to any "red flag" characteristics of a customer.

Adapt to changing risks

Intelligent and organized criminals are constantly probing AML systems to discover new techniques to move their funds. Risks also change as a bank expands into new markets or adds products and services, and as regulators increase their expectations.

Banks that have implemented first-generation AML solutions often find it difficult to evolve these systems to keep up with changing requirements. Many banks have been hit by formal enforcement actions—fines or business restrictions—for AML program shortfalls. Others have expended significant resources on vendors and consultants to force-fit new scenarios onto old, static systems. Before being judged insufficient at the next round of regulatory review, financial institutions need a better way to adapt their scenarios and risk factors to a changing world.

Toward a new model of detection and prevention

To address these challenges, most financial institutions have implemented some form of automated AML system to recognize unusual patterns in transaction activity, and to assess the risks posed by different types of customers and transactions.

A number of niche vendors offer basic transaction monitoring systems that offer limited detection abilities. These systems use basic “if-then” logic or simply compare account/customer names to government watch lists. These low-end systems generally do not offer an integrated environment for investigating and managing alerts.

Larger financial institutions need more sophisticated solutions, but even with higher-end systems, transparency and scalability can be issues. AML staff might not be able to drill into the logic and transaction history that triggered an alert. The platform must also be flexible enough to adapt to internal and external change. Financial institutions that chose static, packaged systems based on low initial cost of ownership may now find themselves having to replace and retool.

When selecting an AML system, banks should ask:

- “Is the vendor going to be in business for the long haul to support our growth and future requirements?”
- “How well can proprietary niche software support our enterprise risk management initiatives?”

The answers could well determine how the bank fares as requirements change and as institutions wish to adopt a broader financial crimes platform.

SAS® Anti-Money Laundering

SAS Anti-Money Laundering provides an integrated environment for an effective, automated AML program. Going beyond typical transaction monitoring, this system:

- Captures and organizes all customer activity across disparate data sources.
- Monitors that activity against industry-specific indicators of criminal behavior.
- Uses analytically derived indicators of risk, not just simple rules and matches.
- Accurately alerts monitoring staff to potentially suspicious activity.
- Provides a structured environment for investigating and documenting alerts.
- Generates required regulatory reports and supporting documentation.

All of these capabilities are provided in a comprehensive solution built on award-winning SAS data management and analytic capabilities. With SAS Anti-Money Laundering, financial institutions can comply with government regulations while ensuring that best practices are maintained across the enterprise.



The SAS solution provides an integrated environment for detecting, investigating and reporting potentially suspicious activity.

SAS Anti-Money Laundering synthesizes data from currently incompatible data sources on almost any platform and format—such as front-office systems, back-office systems and spreadsheets—into data models designed for AML programs.

The Core aggregates customer profile information and transaction activity into one consistent view of the customer across all business units and transaction/instrument types. This data model stores detail and summary data related to historical customer behavior, such as:

SAS Anti-Money Laundering

- Robust data environment supports all products, channels and LOBs. Point-and-click interface enables easy modification and creation of analytic scenarios.
- Daily scoring of customers' risk based on past, present and expected activity across all accounts.
- Proven implementation methodology gets you up and running in a matter of months.
- Aggregates data from across the institution and beyond. Delivers the broadest perspective on potentially suspicious activity.

- Customer, account and household attributes.
- Frequency, recency and monetary attributes of transactions.
- Activity by time period, customer account, channel and product.

To facilitate time-series analysis and trending, this data model stores multiple months of transaction data. If your institution has already consolidated the requisite information in a data repository, SAS can map directly to the existing repository.

The Knowledge Center is where scenarios and risk factors are defined, user privileges and group membership are maintained, and alerts and investigative activities are documented. All actions, comments, documents and decisions are documented and retained in the Knowledge Center to support independent audit and review.

Identify and rank suspicious activity for investigation, without wasting time and energy on trivial alerts or false positives

The alert engine accesses the data management component to evaluate all daily transactions and other information, such as government watch lists. It then applies rules and scenarios derived from financial institutions and regulatory requirements to detect patterns that are indicative of potential money laundering.

Sophisticated Bayes risk ranking algorithms determine the likelihood that illicit activity could be concealed in any combination of scenarios and risk factors. Alerts that show key risk factors, as determined at each institution, can then receive higher priority. False positives can be identified before they consume unnecessary resources. Companies can fine-tune scenarios, risk factors and business logic based on feedback provided by the system's reports.

The SAS solution goes beyond simple rules-checking, and uses seven key methods to identify potential money laundering:

1. Matches with known money-laundering schemes.

Right out of the box, SAS Anti-Money Laundering identifies more than 64 schemes known to be used by money launderers. Pattern definitions can be adjusted for new lines of business or as financial criminals devise new methods.

SAS continually updates its library of schemes and shares them through our consortium of leading financial institutions. With an open forum and process for sharing scenarios, your institution benefits from the knowledge of some of the world's best compliance organizations. Your in-house specialists can also detect new behavior at any time using a point-and-click interface. With some other solutions, you would need to engage consultants for weeks of custom programming.

2. Matches with internal or external name lists.

SAS Anti-Money Laundering checks customer names against OFAC (Office of Foreign Assets Control) or other “high-risk” watch lists from any internal or external source. A match to an external watch list, such as an Interpol or World-Check list, could be factored into the customer’s risk ranking or automatically trigger an alert. The bank can create and maintain an internal list to track customers they want to monitor more closely (perhaps the bank generated an investigation on that customer in the past) or to avoid spending time investigating trusted entities.

3. Occurrence of high-risk transactional behaviors.

Today, many banks train their investigators to watch for transactions of certain amounts or involving high risk geographies, addressing perhaps 30 or more risk factors. As one can imagine, this approach is labor-intensive and error-prone. If investigators leave, they take that knowledge with them. Furthermore, suspicious transactions entail multiple actions that, taken separately, are not suspicious.

The SAS solution can assess combinations of risk factors—as many factors as you want to include. For instance, you could prioritize alerts for non-resident alien transactions over a certain amount in a wire transfer. Overlapping high-risk transactional behaviors can be considered in concert with high-risk Know Your Customer data and automatically flagged for presentation to investigators.

Authorized administrators can add or change risk factors without having to notify or retrain investigators. Even if there is churn among investigators, everyone has access to the latest risk knowledge because it is embedded in the solution.

4. Match to high-risk KYC/CIP profiles.

Which customers are members of high-risk groups, as defined in the FFIEC manual or by your own risk assessment? What is normal behavior for a policy, account or customer? In order to truly take a risk-based approach, the data collected through Know Your Customer (KYC) and Customer Identification Program (CIP) processes must be used in your transaction monitoring.

SAS Anti-Money Laundering uses CIP data every step of the way. Members of high-risk groups have their own scenarios and risk factors. High-priority alerts involving non-bank financial institutions are routed to an analyst with the proper background to review the activity. Risk factors identifying alerts that involve high-risk groups or elevated CIP scores are labeled to avoid switching between systems, saving time and preventing human error. Management reports then pinpoint the risk factors that lead to costly investigations, providing insight for institutions trying to lower their cost of compliance.

Based on summary profiles of historical transactions, the SAS solution can calculate expected behavior. The system then applies scenarios and risk factors to monitor variances against normal or expected behavior. Examples include dormancy, velocity of funds transfers, increased activity or higher-than-normal transaction value.

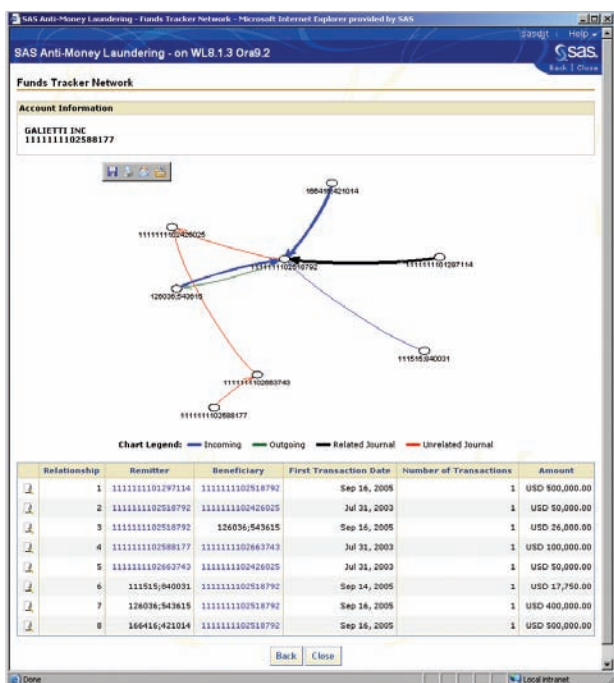
Is this a business that expected to engage in one type of activity, but now is demonstrating entirely another pattern? Has the business deviated greatly from expected deposits or transaction value per month, or from past trends? This kind of insight is a big emphasis for regulators, who expect AML monitoring systems and staff to review and document why actual activities are inconsistent with their customer profiles.

Understanding who a customer says he is, what he has done in the past and what he will do next is a manually intensive task in some systems. The SAS methodology reduces time, cost and the risk of error by integrating the entire process.

5. Suspicious flows of money among accounts.

Criminals are adept at covering their tracks by layering multiple transactions to and from multiple accounts. Money laundering typically involves a complicated series of transactions spread across multiple countries, business entities, accounts and financial instruments. If you could visualize the flow of funds and perform at-a-glance link analysis, complex and ingenious schemes might become apparent.

SAS Anti-Money Laundering has the unique ability to display color-coded maps that diagram the flow of funds among accounts. In one screen, you can see everybody in a customer's transaction sphere and drill down into the map view to see relationships that might be significant. For instance, you might see that seemingly unrelated parties are wiring money to a common recipient, which might warrant a closer look. With this feature, a compliance analyst can “follow the money” in a way that other vendors’ link analysis techniques cannot match.



Track and view the movement of funds among accounts. Blue and green lines indicate flows into and out of the institution. Black and red denote related and unrelated journals.

6. Redundant personal data.

Most banks look for occurrences of duplicate phone numbers, often by manually comparing data from disparate systems. With SAS, investigators have one link that detects many types of shared personal data, such as duplicate names, tax identification numbers, phone numbers, addresses or employers among unrelated parties in the bank’s customer base. For instance, if a social security number (SSN) or Tax Identification Number (TIN) shows up in the record for customers in different households, this anomaly could trigger an alert or be factored into risk rankings.

This capability is particularly important with the prevalence of cell phones. Cross-matched phone numbers could reveal inappropriate, redundant accounts, stolen phone numbers used for illicit purposes, or an unusual number of phone lines for the customer profile.

Related Entities Investigation (Current)			
Customer Information			
ERIC J DERR 999902476776			
Tax ID			
997539949			
Account	1111111102623009	ANTHONY D DONAHUE	
Account	1111111102356867	STEVEN M AMAYA	
Customer	999900254026	JOHN D NIK INC	
Customer	999900263130	KAREN KELLER	
Mailing Address			
1725 MINDOT ST APT 101 MANALAPAN, NJ 07726 USA			
Customer	999902255451	MARTHA ZHU	
Street Address			
1725 MINDOT ST APT 101 MANALAPAN, NJ 07726 USA			
Customer	999901969733	JEAN INC	
Primary Phone			
(111)357-2162			
Household	3006810	TIMOTHY J KEENEY	
Customer	999902963305	DANIEL C HAWK	
Customer	999901148394	DIANA J DERR	
Secondary Phone			
(111)457-2162			
Household	49602	ALAN D JEAN	
Household	37950	VIRGINIA S STEHR	
Customer	999901148394	DIANA J DERR	
Customer	999901662917	RAYMOND T ODANIEL	
Other Phone			
(111)457-1141			
Household	2547184	MARY C SCHMIDT	
Customer	999901148394	DIANA J DERR	
Customer	999903402399	MARY C SCHMIDT	
Employer			
SERAC CORP			
Customer	999901268661	AMANDA MALFITANO	
Name			
ERIC J DERR			
Customer	999903440206	CHERI A NG	

- SAS has created a forum of leading financial institutions to share best practices. Your institution can take advantage of the collective intelligence of these industry leaders, whose insights are built into SAS Anti-Money Laundering.

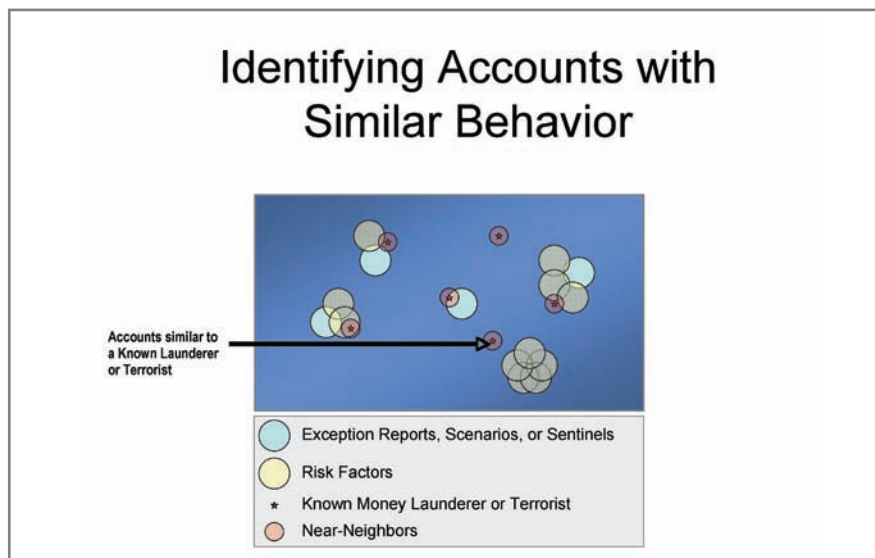
Quickly view related entities and identify duplicate personal data.

7. Reported suspicious activity.

The SAS solution “learns” from occurrences of known illicit behavior, such as prior alerts generated or prior regulatory reports filed. The weightings assigned to scenarios and risk factors are constantly evaluated as the system is used, giving you the confidence to refine your risk assessment and focus your monitoring system on your risks.

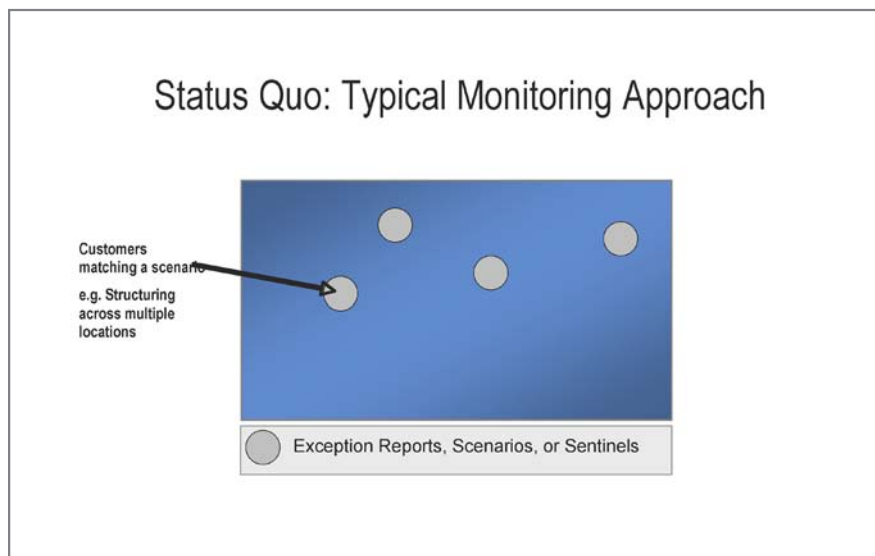
Similarly, the solution can use previous occurrences of known illicit behavior to identify accounts that have the most similar behavior—the “nearest neighbors.” This unique SAS capability is valuable because it detects accounts that might otherwise avoid detection through parameter-based monitoring techniques.

Both types of closed-loop learning help AML programs evolve with a changing customer base and risk landscape.



SAS is unique in being able to identify “near neighbors” to known money launderers.

By using the right detection techniques to sift through mountains of customer and transaction data, the solution increases the chance of detecting criminal activity while reducing the number of false positives.

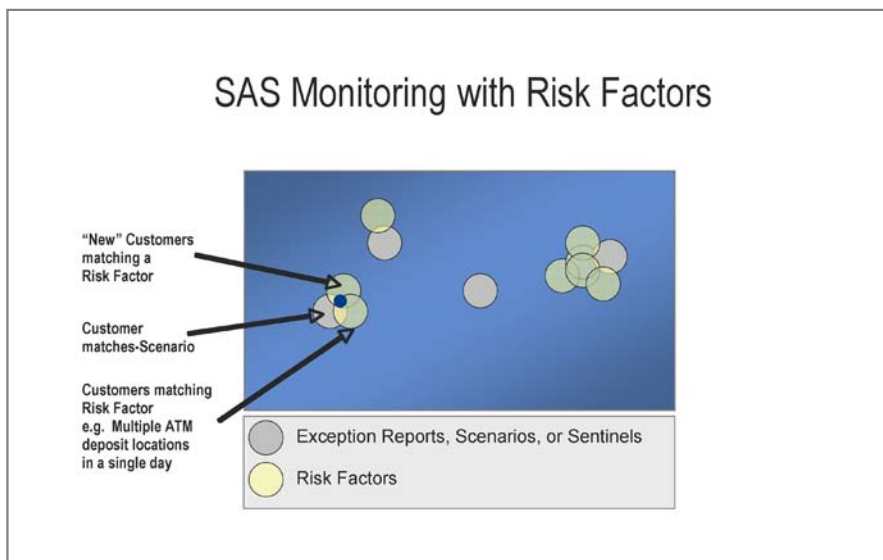


Typical solutions simply monitor transactions and look for rule matches.

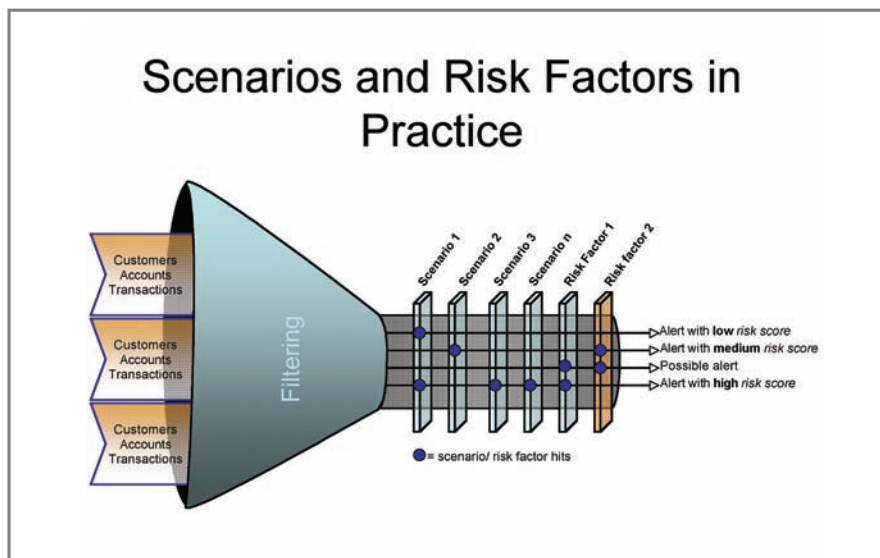
The SAS methodology accurately identifies other cases that rule matching would miss.

Refine rules and scenarios with the click of a mouse

- The SAS solution includes a point-and-click interface for adjusting parameters or even creating your own routines.
- Changes can be tested to reduce false positives and improve the effectiveness of the monitoring techniques.
- The analyst can determine the validity of each rule or scenario and evaluate its effectiveness by seeing how many alerts would be generated under various situations.



The SAS methodology accurately identifies other cases that rule matching would miss.



Some high-risk customers might not be apparent using a single rule, but investigators gain a better perspective of behavior when evaluated across multiple lines of business and risk factors.

If any of these seven key methods identifies activity that could signal money laundering, the solution generates an alert and ranks its significance based on which scenario(s) triggered the alert, other risk factors that apply to the same entity, the likelihood that the alert will result in a regulatory report, and alerts previously generated for that entity. Each alert is assigned a ranking for money laundering risk and terror financing risk. Investigators can then focus their energies on the highest-scored, or most important, alert.

Investigate potentially suspicious accounts or activity

A secure, Web-based interface gives investigators an automated, efficient way to process alerts. This interface presents aggregated profile and activity information in one central location, which saves time and energy. Users can add comments, attach documents, e-mail cases to colleagues, link to previous alerts or file regulatory reports directly from the interface.

When compliance officers/investigators open and process alerts, a system of record is automatically captured. The case file stores comments, attached documents, pertinent dates and actions, etc. With this self-documenting facility:

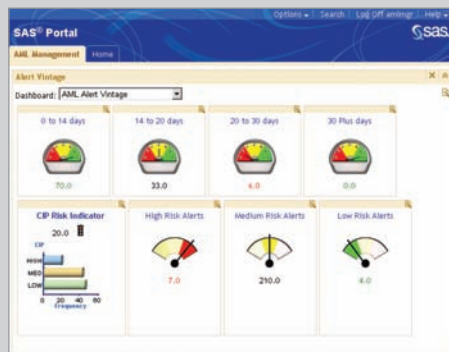
- Management can be sure investigators are following policies and procedures.
- Investigators can focus their energies on processing alerts, rather than documenting their actions.
- All case detail is transferred if the case is reassigned, escalated to a higher level or reopened years down the road.
- The bank can show regulators that every action was governed by established policies, procedures and controls, thereby reducing the risk of legal action, penalties or added scrutiny.

During an investigation, all relevant data is captured in the Knowledge Center data repository. This historical data provides an investigative audit trail and supports continuous self-learning that makes the solution ever-more-effective at predicting suspicious activity and reducing false positives. Administrators can fine-tune user permissions to mirror the roles, security policies and processes of the institution.

- Many financial institutions find the built-in transparency of SAS to be just as valuable as accurate and timely submissions. Unlike “black box” systems, there are no ‘behind the scenes’ activities; every action taken is captured in an audit trail..

Provide senior management with information on key performance metrics

Senior compliance and risk management officers can have real-time access to the key performance metrics of the AML monitoring system. The Web-based portal can provide summary information on the types of alerts generated, staff productivity, geographic exposure and effectiveness of analytic techniques. Providing this information on demand reduces the dependence on information technology staff and insures transparency among stakeholders.



Meet regulatory reporting requirements with automated generation of SARs/STRs and supporting documentation

If an alert warrants reporting to authorities, investigators can launch a secure, Web-based facility to generate files for electronic submission of SAR/STR reports—as well as tracking reports that detail the origin, contents and activity history of each submission. Many fields are pre-populated with information available from the system to increase productivity and reduce the chance of human error.

An investigator can create a new SAR/STR for an alert, save the in-progress form and retrieve it later to work on it some more. Once the investigation is complete, the completed report is flagged for filing. This automated function dramatically reduces the cost of these required reports, which can be as high as \$8 to \$15 per submission using manual methods.

Monitor and manage system access and utilization

In a user-friendly, point-and-click graphical environment, authorized system administrators can manage security and system parameters for:

- **System access**—authorized users/groups and their permissions to use various system functions.
- **Data extract, transform and load (ETL) processes**—source and target data structures, data transformation logic, load parameters and refresh cycles.
- **Alert-generation methods**—scenarios, rules, risk factors and detection models that reflect the most up-to-date knowledge of customers and world conditions.
- **Investigative workflow**—customized rules for distributing the workload to compliance analysts, conducting investigations and making regulatory filings.

Summary

SAS Anti-Money Laundering provides value in many areas:

- Data models designed specifically for money-laundering detection provide an essential, enterprisewide view of customer and account activity.
- Advanced analytic techniques monitor behavior from several angles, including: (A) Deviating from expected, normal activity; and (B) Similar to known suspicious activities—both signaling potentially suspicious behavior.
- Heuristic rules monitor dozens of money-laundering risks that are unique to your institution, its products, services, customers and history.

- SAS Anti-Money Laundering boosts compliance while reducing the cost of achieving that compliance – first, through process efficiency and automation and second, by mitigating the risks of fines, penalties and bad publicity that could result from deficient processes.

- The system visually displays hidden relationships using personal information and transactional activity, so compliance analysts can more effectively identify suspicious relationships.
- Detection and investigation processes are automated in a repeatable and consistent manner. All decisions are documented and archived for audit and regulatory review through a Web-based workflow environment.
- Where necessary, the system automates the generation and filing of SARs/STRs to the appropriate Financial Intelligence Unit.

The monitoring process is transparent, and the entire platform is adaptable to your institution's risk profile. Scenarios and risk factors are driven directly from the bank's AML risk assessment and can be changed easily as risks change for the institution or the industry as a whole.

The SAS Anti-Money Laundering solution has proven its value for financial institutions on every continent with assets from less than US\$2 billion to more than US\$1 trillion, representing all financial sectors. For smaller organizations, SAS offers SAS Money Laundering Detection, which makes the SAS methodology affordable for local and regional banks, savings and loan associations, third-party payment vendors, credit unions, etc.

To find out more about how SAS Anti-Money Laundering and SAS Money Laundering Detection can mitigate regulatory risk while reducing the cost of compliance, visit us on the Web at www.sas.com.

About SAS

SAS Anti-Money Laundering is developed and supported by SAS, the leader in business intelligence software and services—with 3.5 million users at more than 39,000 sites in 110 countries, including 96 of the top 100 FORTUNE Global 500® companies.

SAS software delivers business intelligence for more than 2,300 financial services organizations worldwide, including 97 percent of FORTUNE Global 500 banks. In fact, more than 25 percent of SAS customers come from the financial services sector—representing 34 percent of 2005 revenues. These customers use SAS solutions for cost control, credit analysis, IT administration, risk management, regulatory compliance, portfolio analysis, Internet channel analysis, customer relationship management and more.

In the last six years, SAS has invested heavily in risk intelligence, featuring solutions for operational risk, credit risk management, Basel II compliance, fair lending, fraud detection and anti-money laundering.

SAS can help you:

- Monitor your institution's unique risks by tailoring your data environment and analytic scenarios to match your risk assessment.
- Implement a risk-based AML program that gives investigators a daily prioritized list of work items based on behavior- and analytic-based risk ratings.
- Get up and running fast with a proven implementation methodology that enables you to meet your deadlines and budgetary requirements.

For banks with limited IT staff and resources, SAS also offers a hosted solution with all SAS-owned technology. You simply provide the data. We, in turn, run it through your chosen scenarios and provide your investigators with highly qualified alerts that they can manage via an online workflow tailored to your unique business needs.

Only SAS offers leading data integration, intelligence storage, advanced analytics and traditional business intelligence applications within a comprehensive enterprise intelligence platform. Since 1976, SAS has been giving customers around the world THE POWER TO KNOW®.



**THE
POWER
TO KNOW.**

SAS Institute Inc. World Headquarters

+1 919 677 8000 Sales +1 800 727 0025 www.sas.com/offices

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. Copyright © 2007, SAS Institute Inc. All rights reserved. 102886_441535.0407