



SAS® Money Laundering Detection

A dynamic, risk-based solution for identifying, investigating and reporting suspicious patterns of behavior

SAS®9

Table of Contents

- Executive summary 1**
- A social and regulatory imperative 2**
- The dilemma for small to mid-sized financial institutions 3**
 - “How can we tackle this enormous responsibility with the processes and controls we have in place currently?” 3
 - “How can we document the decision process for regulatory review?” 3
 - “How can we possibly investigate everything that appears suspicious with our limited staff?” 4
- Toward a new model of detecting and preventing money laundering 4**
- SAS® Money Laundering Detection..... 5**
 - Start with high-quality data..... 6
 - Identify and rank suspicious activity for investigation 6
 - Implement an automated, fully documented system for investigative review..... 8
 - Look deeper into alert cases with ad hoc analysis 8
 - Meet regulatory reporting requirements..... 8
 - Monitor and manage system access and utilization 9
- Get up and running fast with a comprehensive solution 9**
- From SAS, a leader in business intelligence for financial services 10**

The content providers for this paper were David Stewart, Program Manager, Anti-Money Laundering, SAS; Tim Lutz, Financial Behavior Expert, SAS; and Sascha Schubert, Product Manager, Data Mining, SAS.

Executive summary

Money laundering has far-reaching implications. It makes organized crime pay. It allows drug traffickers and smugglers to expand their operations. It undermines government tax revenue and the financial community in general, because it siphons vast sums of money from national economies. The events of September 11 added even more incentive to stem the flow of illicit funds.

To identify and prevent this activity — and to meet regulatory mandates — large global financial institutions have deployed high-end anti-money laundering (AML) software, such as SAS Anti-Money Laundering. This sophisticated, risk-based monitoring and alert system detects the subtle patterns that could indicate suspicious behavior.

Now, robust SAS anti-money laundering methodology is available in a solution tailored for small to mid-sized financial institutions — affordable for local and regional banks, savings and loans, money services businesses, insurance companies and credit unions.

SAS® Money Laundering Detection provides automated processes for detecting, investigating and reporting suspicious behavior. Unlike other solutions targeted for this market, the SAS Money Laundering Detection solution:

- Applies a risk-based approach recommended by the Federal Financial Institutions Examination Council (FFIEC) and the Financial Services Authority (FSA).
- Applies multiple, customizable methods for identifying alert conditions against large volumes of financial transactions.
- Supports an automated, fully documented alert management process for investigating and managing suspicious cases.
- Provides a complete view of customer activities across all accounts and transactions.
- Automates the creation and submission of reports to regulatory agencies, such as Suspicious Activity Reports (SARs).

Small to mid-tier financial institutions now have a proven, effective way to identify and track suspicious behavior based on complex statistical patterns, not just simple “if/then” rules and account name lookups. With this solution, banks can effectively capture and organize all customer activity, monitor that activity against a set of industry-specific indicators of criminal behavior, investigate and document suspicious cases and produce required regulatory reports — all within an integrated solution that leverages the power of award-winning SAS data management and analytic capabilities.

A social and regulatory imperative

- A tourist walks into a casino, buys a mountain of chips with cash, gambles conservatively for 30 minutes or less, then cashes out all the remaining chips.
- A bank customer deposits a series of checks into a personal checking account, each one just under \$10,000.
- An entrepreneur sets himself up as a real estate developer, invests heavily in land for building lots, then reinvests large sums of money without building any homes.
- A Good Samaritan sends a generous donation to a charity, which in turn uses it to buy provisions from obscure suppliers that do not seem to be traceable.

In these particular examples, the tourist was turning ill-gotten gain into casino-gotten cash. The bank customer was evading the attention of the Internal Revenue Service. The entrepreneur was growing cannabis, not condos. And the Good Samaritan was funding terrorism, not charity.

Criminals and terrorists have been resourceful and persistent with their money-laundering — an activity that accounts 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 for subversive activities. The USA PATRIOT Act, signed into law the following month, expanded the definition of “financial institutions” and the requirement to detect (and report) suspicious activity that may be indicative of money laundering or terrorist financing. So did the Second European Directive and other AML regulations enacted around the world.

Under the 1970 Bank Secrecy Act, financial institutions in the U.S. had already been required to report cash transactions of \$10,000 or more to the U.S. Treasury department. All anti-money laundering legislations amended after September 11 expanded the scope of accountability to a broader range of businesses, not just banks — such as brokerages, insurance firms and money services businesses. It also holds these businesses accountable not only for detecting money laundering, but for preventing it.

The consequences can be serious, from stiff penalties and fines to costly legal battles, jail terms and loss of business reputation. Just ask Riggs National Bank, which was hit with a \$25 million civil penalty for having deficient internal controls and suffered even greater losses to shareholder value. Or ask the European bank that was assessed a \$100 million fine for allowing improper transactions. Or the international bank that had licenses withdrawn for four Japanese offices for engaging in private banking. And lest anyone think low-profile, domestic institutions are under the radar... a southeastern bank faced \$50 million in fines for charges that it didn't file appropriate suspicious activity reports (SARs).

“With its reporting rules and due diligence requirements, [anti-money laundering] compliance has always been a thorn in the side of banks everywhere,” stated an Aberdeen Group, Inc., white paper (Anti-Money Laundering Software: On Electronic Patrol – 2002). “With the increased emphasis on AML, the pain universe has expanded.”

The recent cases make it clear that all institutions — even community and regional banks, and credit unions — must implement anti-money laundering programs. “Given the current political and regulatory climate, banks have little choice but to shoulder the new compliance burdens,” wrote Karen Epper Hoffman in *Banking Strategies* (January/February 2005). “Given this heightened regulatory scrutiny, the larger scope of banks' responsibility and the ever-greater possibility for financial penalties, it's no surprise that banks are doubling up their investment in staffing and systems for AML prevention and detection.”

The dilemma for small to mid-sized financial institutions

Now that most of the top 20 financial institutions have implemented anti-money laundering systems, some analysts believe that money launderers will turn to smaller financial institutions where information systems may be less sophisticated.

This possibility raises concerns for the risk and compliance officers in these smaller institutions, with good reason. They're asking some tough questions...

“How can we tackle this enormous responsibility with the processes and controls we have in place currently?”

It's not easy to identify money-laundering practices. Money laundering, by definition, is designed to be covert and leave no trail. If someone is seeking to disguise the illegal origin and criminal nature of huge amounts of money, they're going to apply some ingenuity to the scheme. Money laundering typically involves a complicated series of transactions spread across multiple countries, business entities, accounts and financial instruments.

Manual processes for detecting suspicious activity are time-consuming and error-prone. There may not be enough staff to perform the required analysis and file SARs in a timely manner. Inappropriate patterns and transactions can easily be overlooked, leaving the institution exposed to greater regulatory scrutiny and corrective action.

“How can we document the decision process for regulatory review?”

Many smaller institutions do not have formal policies or capabilities in place for documenting their review decisions and managing that documentation. If regulators don't have faith in the consistency and accountability of an institution's procedures, they will watch even more closely.

The process is already burdensome enough. If data isn't aggregated, it can be hard to get information together for the auditors. Investigators may lose information and have trouble tracking activities — especially if a case passes through several investigators' hands. SARs must be manually produced. As a result of all these delays, reports get filed late, introducing the risk of fines and other legal action.

“How can we possibly investigate everything that appears suspicious with our limited staff?”

Anti-money laundering regulations mandate a program of prevention and identification, but they don't require this system to be automated. So it would be natural for institutions to try to assemble a program that cobbles together existing systems with manual intervention. However, banks that try this approach quickly find themselves overwhelmed.

Investigators spend too much time looking for information and documenting their actions — yet they still have a hard time tracking what has taken place in an investigation. The sheer volume of alerts may be more than investigators can manage. If they can't distinguish high-risk transactions from low-risk ones, they will be unable to meet the regulatory expectations of a risk-based anti-money laundering program.

You could hire more investigators, but at what cost? Some institutions respond by filing extra SARs “just in case.” This happens so often that regulatory agencies are already grouching about “defensive filing” of trivial reports.

Toward a new model of detecting and preventing money laundering

To address these challenges, financial institutions need enterprisewide systems that protect against regulatory risk while enabling more informed decisions about potentially suspicious customer behavior.

“There is some relief available in the form of more sophisticated transaction monitoring systems, which do a better job of recognizing unusual patterns in transaction activity and rating customers and transactions by risk levels,” wrote Hoffman in *Banking Strategies*.

The advantages of such a system are self-evident, but finding the right solution has been more elusive. A number of niche vendors deliver basic systems designed for the small to mid-tier market, but they tend to offer limited detection abilities. They use basic “if-then” logic or simply compare account/customer names to government blacklists.

Low-end systems generally do not offer an integrated environment for investigating and managing alerts. And they typically provide limited monitoring of account transactions. With such a solution, upfront cost might be low, but the ability to satisfy evolving requirements is unlikely.

Even if very basic capabilities were seen as sufficient, institutions would also have to ask: “Is the vendor going to be in business for the long haul, to support our growth and customization requirements?” and “How well can proprietary niche software contribute to our overall performance intelligence architecture?”

“Solutions based on transaction filters can help stop the most egregious forms of money laundering, but corporations cannot stop there,” stated the Aberdeen Group white paper (Anti-Money Laundering Software: On Electronic Patrol – 2002). “Sooner or later they must adopt more sophisticated solutions that not only offer more technological power, but also are more effective at being integrated into the day-to-day logistics of regulatory compliance.”

But what are the options? Historically, full-featured anti-money laundering programs designed for large global institutions were out of the reach of regional or local banks. Until now.

SAS® Money Laundering Detection

The SAS Anti-Money Laundering solution is deployed in large global institutions, such as Bank of America and Morgan Stanley — and in mid-sized institutions, such as BB&T, First Citizens Bank and Sovereign Bank. SAS now offers a complementary version of this solution for small to mid-tier banks.

SAS Money Laundering Detection provides robust, SAS anti-money laundering methodology in a solution tailored for local and regional banks, insurance companies, casinos, money services businesses, and other financial services companies. This integrated solution provides automated processes for detecting, investigating and reporting suspicious behavior. Unlike other solutions targeted for this market, the SAS solution:

- Applies a risk-based approach to monitoring customer behavior.
- Supports an automated and self-documenting alert management process for investigating suspicious cases.
- Auto-generates SARs (suspicious activity reports) for regulators, in addition to customized reports.

This comprehensive, end-to-end solution makes it possible to unify business entities and establish sustainable, repeatable best practices across the organization. As such, smaller institutions now have a proven, effective way to ensure regulatory compliance as well as protect shareholder value and brand reputation.

With SAS Money Laundering Detection, small to mid-tier financial services companies have a new option — a Lexus system at a Toyota price... a system that was originally developed for the largest global financial institutions, now scaled and priced for small to mid-sized financial services institutions.

SAS Money Laundering Detection components

- Data management
- Reporting
- Alert generation and management
- Analytics
- Administration

Data management

- Money laundering data model and data mart
- ETL routines to aggregate all data sources
- Complete software suite for accessing, scrubbing and managing data
- Scalable data management capable of assessing large amounts of transactions daily

Start with high-quality data

The SAS solution synthesizes data from currently incompatible data sources on almost any platform and format — such as front-office systems, back-office systems and spreadsheets — into a data model designed for money laundering detection. Data cleansing and validation capabilities deliver timely and accurate data.

You can aggregate customer profile information and transaction activity into one consistent view of the customer across all business units and transaction/instrument types. The solution can read government and third-party watch lists and match this information against your internal data.

With a high-quality data repository, you can have confidence in the quality and integrity of reports, submission data and the business decisions that result.

Alert generation and management

- Library of prebuilt scenarios and risk factors
- Ability to modify/create your own scenarios
- Risk-ranked alerts based on customer behavior provides context for investigation of alerts
- Watch-list scenarios to monitor transactions against high-risk lists using fuzzy-matching algorithms

Identify and rank suspicious activity for investigation

Relieved of burdensome data management tasks, investigators can now devote their time to proactive analysis and productive “what if” investigations — distilling business intelligence from the masses of data collected and summarized for compliance purposes.

The SAS solution goes far beyond simple filtering and profiling, far beyond simply comparing customer names to suspect lists (which it also does). Right out of the box, the solution includes more than 50 built-in scenarios and risk factors to identify suspicious accounts or activity. You can modify the standard templates and create new ones to reflect your proprietary knowledge of your products and markets.

By using multiple detection techniques that can sift through mountains of customer and transaction data, the system increases your chances of detecting suspicious activity while reducing the number of false positives. You can then rank suspicious behaviors based on any number of risk factors that have been derived from leading FIUs.

The SAS risk-based approach enables you to assign weights to certain factors — such as new customers, foreign wires, cash equivalents, etc. — so alerts will be scored according to the likelihood of wrongdoing. Investigators can then focus their energies on the most important alerts. Automated risk scoring fortifies the AML programs of the most sophisticated financial institutions. Now, with SAS Money Laundering Detection, this effective technique can be deployed easily in smaller institutions.

A risk-based approach to anti-money laundering

Realistically, a financial institution cannot detect all instances of wrongdoing by customers, but if there are systems and procedures in place to identify higher-risk customers and transactions, you're a step ahead. At the very least, you can focus your energies on the most likely cases.

How do you ferret out the "most likely" cases? Skilled money launderers know abnormal behavior will attract attention and adjust their transactions accordingly. However, there are characteristics of money laundering and terror financing that cannot be hidden by simply changing the sequence, amounts or types of transactions. Event-based detection methods would miss these subtle indicators.

That's why the Financial Action Task Force (FATF), the USA PATRIOT Act and new European Union directives all recommend dynamic risk-based analysis. Large institutions have embraced risk-based methods, but this approach has typically been unavailable in solutions for small to mid-sized institutions. Most basic money laundering systems only offer simple filtering and comparison of names to blacklists.

With risk-based controls in SAS Money Laundering Detection, you can monitor risks associated with:

- Country — Does the transaction or customer originate in a country that is not a FATF member, is politically unstable, has widespread drug production or deficient AML controls?
- Product — Some products carry higher risk simply because the bank tends to collect less background information, such as personal checking accounts. Others, such as securities, are higher risk because they are widely favored for money laundering or terrorist financing.
- Entity — Does the account represent a political figure, a person with past suspicious activity or an entity that could veil a money launderer's true identity, such as a nonprofit organization?
- Behavior — Does the customer show certain behaviors that are related to higher risk, such as frequent use of high-risk financial instruments or velocity of transactions.

SAS Money Laundering Detection applies sophisticated risk-ranking algorithms to assess risk at the customer level. This technique is far more effective than scoring individual transactions and accounts. For the investigator, they are provided with a holistic risk assessment.

Implement an automated, fully documented system for investigative review

Risk factors provide investigative context for explaining why one customer represents a higher risk than another.

Using a self-documenting system to process those alerts enables investigators to focus on investigation instead of documentation.

A secure 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. The Administration component ensures that this process mirrors the roles, security policies and processes of the institution.

When compliance officers/investigators open and process alerts, an audit trail records every step of the decision-making process. The case file stores comments, attached documents, pertinent dates and actions, etc. With this self-documenting facility:

- Management can be sure investigators are applying consistent and approved best practices.
- 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 procedures and controls, thereby reducing the risk of legal action, penalties or added scrutiny.

Look deeper into alert cases with ad hoc analysis

Compliance staff frequently need to be able to look beyond the superficial when investigating cases. With the SAS ad hoc reporting and analysis tool, SAS Enterprise Guide, authorized users have read-only access to virtually the entire data repository, using a graphical user interface.

SAS Enterprise Guide allows a business analyst to “drill down” into detail and dissect data on many dimensions. Investigators can assess the real statistical significance of results, diagnose false-positive findings and isolate patterns for further investigation. Every step of the ad hoc analysis can be viewed, validated and audited.

Reporting

- Query and reporting interface to see transaction details and generate reports
- Ability to track relationships on account and customer level
- Ability to populate SARs
- Default reports and ad hoc reporting

Meet regulatory reporting requirements

The SAS Money Laundering Detection solution generates correctly formatted files for electronic submission of SARs to regulatory agencies — as well as tracking reports that detail the origin, contents and activity history of each submission. This process improves efficiency and reduces the likelihood of human errors.

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 reflected in a log.

Monitor and manage system access and utilization

Given the importance of securing your money laundering detection system, the SAS solution enables you to regulate which individuals can access the solution and what they can do with it. Global system parameter tables define the profiles of authorized users and their permissions to use various functions, such as system administration, data management, alert investigations, internal Web reporting and external report submissions.

With this flexible solution, authorized users can modify system parameters — such as scenarios, risk factors and detection models — so the system always reflects the most up-to-date knowledge of customers and world conditions. Audit tables track all system administration activity, including a before-image of any changed record and detail about who made the modification and when.

Administration

- Manage rights and privileges based on user profile.
- Create and modify scenarios and risk factors to meet specific requirements.

Get up and running fast with a comprehensive solution

With a “Quick Start” implementation methodology, SAS Money Laundering Detection can be implemented within 90 days in standard cases, thanks to several design features:

- A prebuilt data model designed specifically for money laundering detection.
- Standard data extract, transform and load (ETL) processes for financial services applications.
- More than 50 prebuilt scenarios and risk factors, created by leading compliance departments around the world.

SAS has created a consortium of leading financial institutions to share best practices for identifying suspicious customer behavior. Your institution can take advantage of the collective intelligence of these industry leaders, whose insights are built into the SAS Money Laundering Detection solution.

SAS Money Laundering Detection is the only solution for small to mid-sized financial services institutions that:

- Combines the knowledge of known patterns of money laundering with a risk-based approach to assessing customer behavior.
- Prioritizes alerts based on the aggregated risk that each customer represents to your institution.
- Enables flexible creation and tuning of scenarios to address risks unique to each institution.
- Integrates into other SAS solutions for banking intelligence, such as risk management and customer intelligence.

SAS® Money Laundering Detection

While supporting best practices in compliance, SAS Money Laundering Detection reduces the total cost of 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. In short, a SAS Money Laundering Detection solution is an investment that pays sure dividends.

With nearly three decades of continuous profitability and annual revenues of more than \$1 billion and growing, SAS has the depth of resources to sustain excellence in product development and customer support — even when lean economic times forced other vendors to compromise or consolidate.

From SAS, a leader in business intelligence for financial services

SAS Money Laundering Detection is developed and supported by SAS, the world's largest privately held software company, with 3.5 million users at more than 39,000 sites in 110 countries. More than 2,000 financial services organizations worldwide, including 97 percent of Fortune Global 500 banks, count on SAS for *The Power to Know*®.

In fact, more than 25 percent of SAS customers come from the financial services sector. They use SAS solutions for risk management, credit analysis, IT administration, regulatory compliance, portfolio analysis, Internet channel analysis, customer relationship management and more.

For more information, visit us on the Web at www.sas.com.



World Headquarters
and SAS Americas
SAS Campus Drive
Cary, NC 27513 USA
Tel: (1) 919 677 8000
Fax: (1) 919 677 4444
U.S. & Canada sales:
(1) 800 727 0025

SAS International
PO Box 10 53 40
Neuenheimer Landsr. 28-30
D-69043 Heidelberg, Germany
Tel: (49) 6221 4160
Fax: (49) 6221 474850
www.sas.com