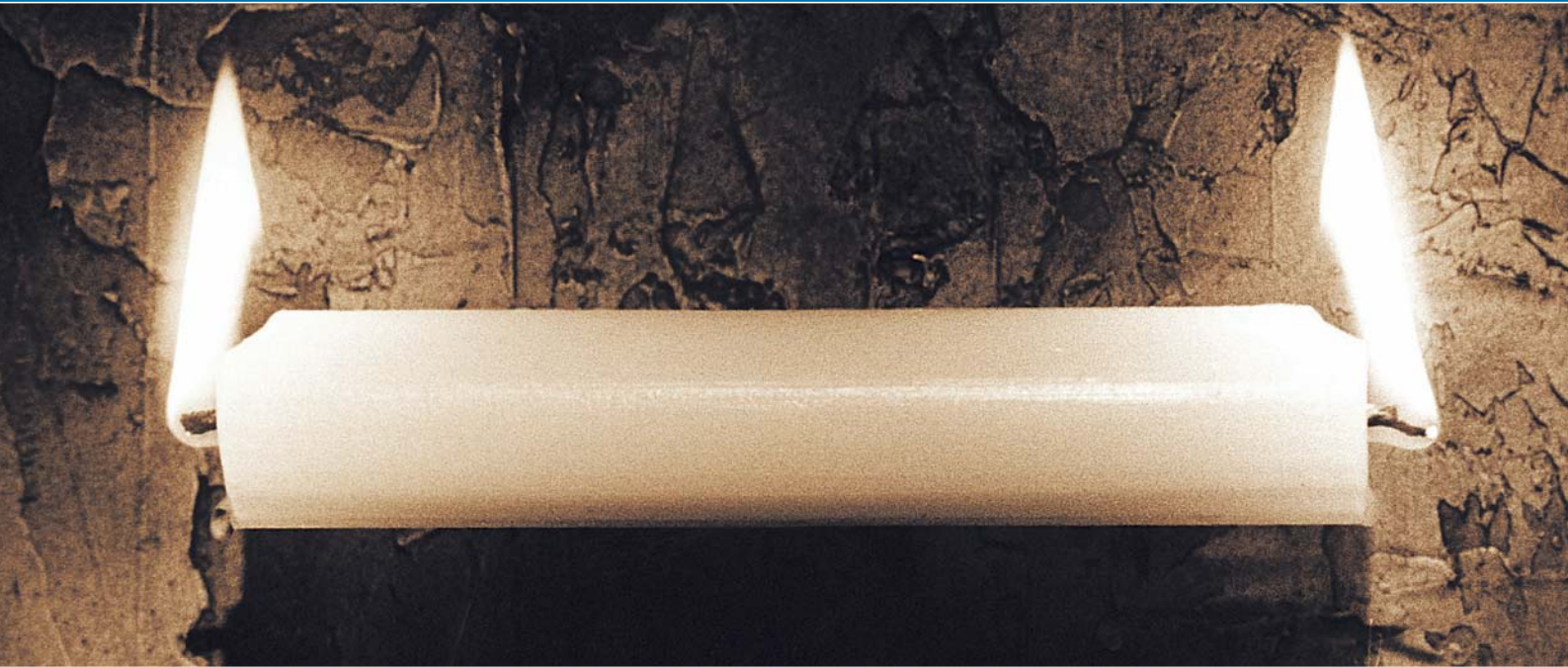


SAS, the leader in business intelligence software, challenges...

Regulatory compliance. Shareholder value. Are you delivering both?



OPERATIONAL RISK

CREDIT RISK

REGULATORY COMPLIANCE

MARKET RISK

FRAUD PREVENTION

Basel II. Sarbanes-Oxley. EU Money Laundering Directive. Regulatory requirements keep growing. So do stakeholder expectations. And both are forcing you to gain a new understanding of every part of your business. SAS® software delivers that enterprise view, combining nearly three decades of analytic accuracy and market leadership in one incomparable risk intelligence suite. So you can adapt quickly to regulatory and stakeholder demands. To learn more about SAS, and our real-world successes, visit our Web site.

www.sas.com/risk

With SAS® you can aggregate data in any volume from across your enterprise. Model and predict likelihood and impact. And approach risk and compliance challenges with consistency and proven reliability.

SAS®9

The Power to Know.®

sas®

Towards a better understanding of the role of technology for ‘best practice’ in anti-money laundering compliance



Rowan Bosworth-Davies M.A.

Director – Fraud and Anti-Money Laundering, SAS EMEA

Much discussion has been generated on the definitions and the application of so-called ‘artificial intelligence’ models, or more commonly ‘intelligent systems’ for detecting money laundering. First of all, it is an oxymoron to describe such offerings as providing ‘detection’ capabilities. They cannot do this. Business intelligence systems can provide a platform for the support of a legal and regulatory case for determining ‘best practice’, but suggesting that technology alone can replace the entirely human decision-making process is to miss the point of the problem.

Demonstrating a high standard of ‘Know Your Customer’ intelligence gathering is an on-going requirement, and is crucial to the provision of effective ‘suspicious’ transaction disclosure. How can any practitioner properly demonstrate ‘best practice’ adherence to the ability to disclose ‘suspicious’ transactions, unless he can show that he has a full knowledge of his customer, his business, his financial profile and his future ambitions, upon which basis the practitioner can then form a meaningful judgement about his client’s activities?

Identifying suspicious transactions is itself, a wholly subjective decision, a feature of the legislation which has always proved to be a major stumbling block in creating a level playing field in compliance procedures. Suspicion is purely subjective, and what makes one person suspicious, may not apply to another. This will remain true, regardless of whether governments (such as the UK or South Africa) seek to impose objective standards of suspicion. In these cases, the court will still need to prove the absence of a subjective judgement before going on to test whether the objective (or non-personalised) standard of suspicion should have been identified.

Trying, therefore, to model a series of activities, which can in any way be said to reflect accurately pre-determined suspicious characteristics, for anti-money laundering ‘best practice’, upon which Money Laundering Reporting Officers (MLROs) can rely with sufficient accuracy, is only of limited value. We can only determine, with the benefit of hindsight, that any particular activity is laundering-specific, because it is a system that has been identified in the past, and has now been exposed. Professional launderers do not make a habit

of using techniques and methods which are already well known to regulators and law enforcers, and they adapt their techniques accordingly.

Ironically, money launderers do not need to take a great deal of trouble in changing their tactics, because the whole concept of money laundering is incapable of specific definition, in any event. Money laundering is merely the egregious use of the world’s commercial, professional, transactional payment and financial delivery systems to move criminally-tainted money. Remaining as closely as possible to traditional payment routes; and maintaining ordinary commercial transactional activity is the best defence against being uncovered as a money launderer.

It is perfectly possible to take two entirely identical sets of transactions, withdraw the proceeds from the same bank account, move them through the same financial products, channel them through the same lawyer’s client account, use them to purchase the same financial investments, and then liquidate their proceeds and route them through the same offshore jurisdiction, to reappear in the same end-user bank account, and one could be a criminal transaction and one could be a legitimate one. The only way to determine either is by knowing the original provenance of the money, and that is predicated upon being able to demonstrate a practical application of KYC procedures.

The most that any business intelligence provider can hope to claim is that they offer a solution, which can assist the MLRO function to aid his or her department’s attempts to achieve a high standard of ‘best practice’. No product offering should claim a ‘detection’ capability, or refer to its findings as ‘suspicious’, because that immediately would put the user into a legal and regulatory difficulty. If the user were to both philosophically and semantically accept that the IT system is really ‘detecting’ suspicious transactions, then he or she is immediately faced with the need to disclose all such reports immediately, in the absence of any further examination or evaluation.

The primary focus, for the demonstration of ‘best practice’, is that the approach adopted must be ‘risk based’ and proportionate to the risk, which means first analysing and identifying the level of risk to be managed by each client. If financial institutions are now to be faced with the likelihood of paying significant sums of money for IT systems which may not even provide them with the ability to do any better than they were doing already, to say nothing about failing to provide them with a requisite return on investment, then they would be forgiven for demonstrating a wilful reluctance to consider any such applications at all.

A practicable rules-based system, with a proportionate capability to provide a robust form of data-mining to manage the on-going transaction monitoring requirement; and coupled with a very user-friendly workflow management offering solution should be the first stage institutions need to consider development for compliance. Such rules need to be capable of being flexibly defined in the

widest possible business environment, so that such a solution can be applied in the widest variety of financial applications.

The primary need is to identify 'unusual' transactions which are exceptions to the ordinary rule of the customer's 'normal' business pattern of activity. Once identified, those exceptions need to be analysed to ascertain whether they really are 'suspicious' as far as the MLRO is concerned, or whether they are merely unusual within the overall pattern of customer behaviour, but still capable of rational explanation. In most cases, and using a 'risk-based' approach, the vast majority of such exception transactions should not create a huge amount of 'noise'. A 'risk-based' approach allows practitioners to start from the perfectly reasonable premise that their customers are law-abiding citizens whose usage of their banking systems will be correct, normal, and unremarkable. Identifying a pattern of exception transactions when set against the 'normal' conduct of the account is not complicated and can be easily achieved through the use of existing, robust predictive analytic systems.

Once relevant exception transactions have been identified, such limited activities can then be tested by a rules engine to ascertain which specific rules have been broken, and if necessary, what actions can or should be further taken, to ascertain whether such a transaction needs to be disclosed. It is in the definition of these rules that the expertise of the application and its architect come into their own. Rules will have to be constructed differently depending upon jurisdiction and geography and regulatory regime requirement. What will apply in the UK will not necessarily work in other countries. US requirements, particularly their routine BSA and SAR reporting, are almost always inapplicable in non-US jurisdictions, except in those cases of financial institutions which are subject to US oversight. Installing US-style regulatory requirements in non-US financial regulatory applications is both additionally cost-intensive and culturally unattractive. There are other ways of ensuring that a non-US bank does not fall foul of US extraterritorial ambitions.

Financial practitioners constantly reiterate the need for simplicity and limitation on the number of rules which they want to see applied. The risks which are being managed are the institution's risks, and they should be capable of defining the level of awareness and management which they wish to bring to the application. Therefore, all rules should be capable of being calibrated with risk weightings, so that the individual institution can 'fine tune' them to their own requirements. The aim is to be able to permit the institution to manage only those transactions which give it greatest cause for concern, and not to force it to have to deal with a whole load of irrelevant 'noise' on the screen. Every exception report generated will have to be examined, it will not be possible to ignore some reports and focus on others. Therefore, the primary need is to be able to calibrate the rate of 'hits' with which the institution wishes to deal. As long as this is firmly and clearly written into the risk profile of the institution concerned, and documented accurately and discussed and understood by the regulator, there is no need to create unnecessary exception reporting.

Based on SAS's industry experience gained from working with over 600 European banks we acknowledge there is no 'one size fits all' application in this market. Each institution is different; has different philosophical approaches to its view of the market; has different risk-management practices and different compliance solution needs. Thus the need is for maximum flexibility, so that the institution can remain completely in control of its own risk management, which can be calibrated in accordance with its own risk management and compliance policies.

Financial services institutions need solution providers who clearly understand the key AML issues and can accurately determine what level of product offering will be commensurate with the institution's immediate needs. This starts with the provision of an absolutely basic solution kit, complete with a minimal number of rules, to which the customer must agree at the start. There will be a minimal amount of pre-scoping and post-sale implementation costs. Once the system is installed, and working satisfactorily to the institution's needs, other rules, and further refinements can be

added at a later stage, once the user has actively demonstrated to their management that such products are not 'business-prevention' systems.

Our customers have repeatedly demonstrated that they do not want pure consultancy-led offerings, because of the unquantifiable level of costs. Those who do not understand this basic issue will simply not succeed. Anti-money laundering solutions should be simple to use, simple to operate, and should not have to involve disproportionate capital expenditure. They are not looked upon with any degree of optimism by most institutions, and those who seek to provide them must demonstrate that they have both significant domain expertise in AML understanding of best practice, and are capable of delivering products at a competitive, cost-effective price.

Anti-money laundering systems should be seen as nothing more than basic solutions which allow financial institutions to be able to know their customers better. In so doing, they can be better seen in their rightful context, which is really as an extension of their Customer Relationship Management solutions. Once this idea is grasped, and their value better understood, then institutions will be more willing to extend their AML solution to core areas such as Fraud Detection and Prevention as well as leverage valuable input into Customer Intelligence and management reporting systems. With this broader integration the AML solution will be seen to demonstrate a far better return on investment than would have been originally identified.

Money laundering is a regulatory risk, and financial institutions are experts at managing risks. An anti-money laundering solution should assist in the management of that risk, it should not become a bigger problem in itself.

About the Author

Rowan Bosworth-Davies (MA), Director, Money Laundering & Fraud Solutions, at SAS, is a leading international expert in education and consulting services in the field of fraud prevention and anti-money laundering awareness programmes. Mr. Bosworth-Davies is the author of a wide variety of books and other AML publications.

Contact Rowan.Bosworth-Davies@eur.sas.com or visit us at <http://www.sas.com/industry/banking> to find out more about SAS' Anti-Money Laundering solutions

About SAS

SAS is the market leader in providing a new generation of business intelligence software and services that create true enterprise intelligence. SAS solutions are used at more than 40,000 sites – including 96 of the top 100 of the 2003 *Fortune* Global 500 – to develop more profitable relationships with customers and suppliers; to enable better, more accurate and informed decisions; and to drive organizations forward. SAS is the only vendor that completely integrates leading data warehousing, analytics and traditional BI applications to create intelligence from massive amounts of data. For nearly three decades, SAS has been giving customers around the world *The Power to Know*.®