Rowan Bosworth-Davies joined SAS EMEA in 2004 as the Director of Anti-Money Laundering and Fraud Solutions. He has more than 25 years of practical and theoretical experience in the investigation and prosecution of fraud and white-collar crime. He has provided training and compliance programs for the Bank of England, the U.K. National Criminal Intelligence Service, the National Police Staff College, Bramshill and has provided consultancy to the Money Laundering Steering Group of the British Bankers' Association.

Anti-money laundering

Toward a better understanding of the use of IT systems for best-practice compliance

Rowan Bosworth-Davies, SAS EMEA

Much discussion has been generated on the definitions and the application of so-called 'artificial intelligence' models, or more usually 'intelligent systems' for detecting money laundering. First of all, it is incorrect to describe such offerings as providing "detection" capabilities. They cannot do this. IT systems can provide a platform for the support of a legal and regulatory case for determining 'best practice', but suggesting that any IT offering 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 ongoing requirement and is crucial to the provision of effective disclosure of "suspicious" transactions. 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 customers, his business, his financial profile and his future ambitions?

Identifying suspicious transactions is itself a wholly subjective process, a feature of the legislation that 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 nonpersonalised) standard of suspicion should have been identified.

Trying, therefore, to model a series of activities that can in any way be said to reflect predetermined suspicious characteristics accurately, and upon which 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. Money laundering is merely the egregious use of the world's commercial, professional, transactional payment and financial delivery systems to move criminally-tainted money. Sticking 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 sets of transactions – one legitimate and one criminal – 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 liquidate their proceeds, route them through the same offshore jurisdiction and have the money reappear in the same end-user bank account. The only way to determine the difference 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 IT product provider can hope to claim is that they offer a tool, 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 would immediately face 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 anti-money laundering 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 clients are now to be faced with the likelihood of paying significant sums of money for IT systems which may not even provide them the ability to improve, not to mention 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 ongoing transaction monitoring requirement; and coupled with a very user-friendly workflow management offering, should be all that most institutions need to consider, certainly in the first stages of development. Such rules need to be capable of being flexibly defined in the widest possible business environment, so that such a tool 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 client'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 client 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 clients 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 data mining 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 comes into its 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 in the number of rules they want to see applied. The risks 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.

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 tool 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 policies.

The issues that need to be considered are what level of product offering will be commensurate with the client's immediate needs. This starts with the provision of an absolutely basic tool kit, complete with a minimal number of rules, which the client must agree at the start. There will be a minimal amount of prescoping and postsale implementation costs. Once the system is installed, and working satisfactorily to the client's needs, other rules and further refinements can be added.

Clients 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 tools should be simple to use, and should not have to involve huge 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 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 tools that allow financial institutions to know their customers better. In so doing, they can be better seen in their rightful context, which is really as client relationship management products. Once this idea is grasped, and their value better understood, then clients will be more willing to consider further additions to the tool kit, at a later stage, and the original offering will be seen to provide a far better management tool than would have been originally identified.

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