Statement of intent

The current accepted wisdom is that businesses need to adapt to a changing environment and adopt a very broad-based approach towards dealing with business risk. Increasingly, global financial regulators are realizing that a great deal more work needs to be done to stem financial crime and there is now a growing focus on the monitoring of every day transactions. Organizations need to be able to identify potentially unusual financial transactions which might subsequently prove to be suspicious within the context of existing anti-money laundering and financial crime interdictions. The mapping of these identifications is critical for a full picture of the client’s business profile, their commercial activities, private wealth distribution and management structure.
ABOUT THE AUTHOR
Rowan Bosworth-Davies is widely recognised as a leading international freelance writer and expert in the field of providing education and consulting services in the field of financial crime, fraud prevention and anti-money laundering awareness programmes.

A legal consultant and a former Fraud Squad detective at New Scotland Yard, he ran the investigations division of one of the UK’s financial Self Regulating Organisations for two years.

He subsequently spent ten years working for two leading law firms in the City of London as a Criminal Justice Consultant. An academic with an Honorary Research Fellowship at the London School of Economics, appointed a Churchill Fellow in 1995, as well as holding Honorary Research Fellowships at Exeter University and the Institute of Advanced Legal Studies, he provides regular lectures to students on white-collar crime issues at UK Universities and law enforcement training centres.

A Master of Arts in Police and Criminal Justice Studies from Exeter University, he has over 30 years practical and theoretical experience of the investigation and prosecution of fraud and white-collar crime.

He is now managing his own specialist writing and consulting practice, providing high level advice and guidance to financial institutions and related companies who need to engage in the areas of financial compliance and financial crime interdiction. After the success of his first book, ‘Too Good To Be True’, Rowan has continued to write and publish extensively. He has published in excess of 400 articles in the past 20 years.
## CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tick Box Approach</td>
<td>4</td>
</tr>
<tr>
<td>A Comprehensive Approach is Critical</td>
<td>4</td>
</tr>
<tr>
<td>Value, Volume and Velocity</td>
<td>4</td>
</tr>
<tr>
<td>Combination of Tools Needed</td>
<td>5</td>
</tr>
<tr>
<td>‘Must-Have’ Capability</td>
<td>6</td>
</tr>
<tr>
<td>A New Broom</td>
<td>6</td>
</tr>
</tbody>
</table>
The realization that more work is predicated in this area has grown out of some of the more recent failings identified in banks observed engaging in active money laundering as part of their ordinary business activities.

Some banks were found to be enabling other foreign banks to avoid the impact of international sanctions; in other cases banks have been heavily penalized for their part in the LIBOR manipulations, and perhaps most worryingly, some institutions were found to have openly engaged in wholesale money laundering.

Regulatory interventions, both in the UK and in other EU countries, reveal that while many institutions have implemented detailed and cost-intensive systems and controls, including IT-delivered software solutions, often these methods have been used to gain a simple tick-box acknowledgement from a regulator rather than to engage in any meaningful identification of suspicious transactions. This practice has attracted criticism from regulators and banking supervisors alike.

Detailed industry research, such as the Thomson Reuters Cost of Compliance Survey 2012, has identified the primary challenges facing compliance officers in a range of global financial services companies. The process of consistently and competently monitoring transaction still demands the lion’s share of the compliance teams’ time.

All too often, the process of identifying suspicious transactions which need to be disclosed to the relevant legal authorities becomes subsumed by the need to perform other duties. This has resulted in a tendency to submit alerts generated by the software monitoring system without the benefit of informed analysis. As a consequence, law enforcement partners are inundated with less than useful information which then requires evaluation.

Transaction monitoring needs to be more than the act of a random ‘data grab’ at any given moment in time, followed by analysis. This will reveal very little relevant intelligence and is merely a snapshot in time.

Proper transaction monitoring requires a systemic and intelligent review of the financial and business activities of each client on a daily basis, 365 days a year, with the appropriate analysis necessary to create a three-dimensional, holistic view of financial behaviour.

Such a process provides for the fullest possible reporting of what each individual client is doing inside their financial activity. It identifies the ‘values’ of the transactions they most usually undertake, both in receipt into the account, and in payment out of the account, thus providing a useful upper and lower parameter for identifying normal activity values.

But such an analysis goes further. It will also measure the ‘volume’ of payments entered into by the client. It will recognize and measure the normal transactionality of the payment traffic over a period of time, a statistic which can be measured and reported on. Such an attribute enables the analyst to establish whether a hitherto normal or usual pattern of receipts and payments have changed or are changing and what the reasons are behind those changes.

Changing transactional patterns, for example, of the client who has normally only cleared a dollar transaction from Latvia on average once every three months, and who for no apparent reason starts to clear a significant volume of dollar traffic from Latvia, may be significant. It may be that their business is growing successfully but it may be that they are clearing many small
payments so as not to raise unnecessary alarms with authorities and the increase in payment volume is because his Latvian client is seeking to move a higher-than-normal flow of dollars from Russia, which might be an issue of concern.

The third element of transaction monitoring which is of relevance is that the system is also capable of measuring the ‘velocity’ of payments moving through the account. By ‘velocity’ we mean the amount of time the incoming money stays in the account before being moved on again. If your client’s normal pattern of business is for a monthly turnover of funds within this account, which might reflect a classic standard personal account responding to a monthly pay cheque and monthly standing order outgoings, then a sudden, dramatic change in a single payment might become a matter of concern. So when a large sum of money is paid into an account and then is almost immediately paid out again in a matter of hours or days, a trigger or alert should go off.

COMBINATION OF TOOLS NEEDED
Such scenarios can be readily identified by using a transaction monitoring product that incorporates the principle of 3V’s – value, volume and velocity. Having the ability to generate these levels of granularity is not sufficient on their own, however, as all these alerts can do is to highlight possible unusual activity, which may prove, on later evaluation, to be suspicious.

This is where having the facility to operate a transaction monitoring process in tandem with an Anti-Money Laundering (AML) screening package provides an extra edge in the evaluation process.

Identification needs more than a name and address. Businesses need to be capable of identifying the client from the perspective of their business profile, their commercial operations, their social and political exposures, and areas of business operation.

It is all very well knowing, for example, the address of a Swiss-based client with a Middle Eastern name, but it is more important to know whether the address is simply a convenient post office box or a substantiated business address.

An effective system would allow you to undertake a screening exercise easily and conveniently without having to move away too far from the screen on which you are working.

To conduct a thorough Know Your Customer (KYC) check you need to know the country of residence, the sector or sectors in which the business is involved, family details, and the Politically Exposed Person (PEP) status. It is also important to know the risk profile of the business, whether it is engaged in import/export from other Middle East countries, who else they bank with, if they have ever come to notice before for issues of concern. All these and many other elements are vital if you are to be able to say that you truly ‘know your customer’.

The ability to engage in detailed AML screening while operating an effective transaction monitoring system provides a powerful compliance tool and minimizes the likelihood of missing an important feature of the client’s business or political profile while analyzing his financial transactionality. These two elements are synergetic of the other so it makes sense to be capable of carrying out both activities in tandem at your desk and without having to break away from one or other activity to cross-reference actions.
‘MUST-HAVE’ CAPABILITY
Such a requirement is now fast becoming a ‘must-have’ capability for professionals. There have been some singular failings in ‘best practice’ compliance actions in recent months and these failures have generated significant debate among regulators both in the EU and in the USA.

Business should take note that in America in particular there is a significant unwillingness to be as forgiving as before when it comes to major failings of compliance.

American regulators and politicians, as well as jurists and prosecutors, are looking more closely at compliance actions and they are measuring the way in which businesses conduct themselves, especially how they respond to US sanctions. Banks who wish to be able to protect themselves from aggressive legal intervention should remember that the US way of measuring compliance effectiveness almost inevitably comes during the plea-agreement process, ie the institution is already staring down the barrel of a prosecution or regulatory process. The prosecutor or official will examine the compliance procedures in use within the bank concerned and will take the effectiveness and efficiency of those processes into consideration when weighing up the penalty.

This of course is not the way of things in Europe, but it would be a foolhardy institution who would believe that it can afford to take such a state of affairs lightly.

A NEW BROOM
It has now become a mandatory exercise for the Director of Compliance in any medium to large-sized financial institution to think about compliance in an holistic way and to find ways of managing the high level of data management and information through-put required to keep a high compliance ‘best practice’ profile.

The times are over when inexperienced professionals with no knowledge of financial crime or banking mismanagement can be hired as AML analysts, given a couple of days training on the IT systems and then left to begin to muddle through. It will not be sufficient if the institution in future finds itself confronted by a major compliance investigation for significant failings, merely to say, ‘well we thought we were just about compliant’.

In the future, regulators are likely to expect the compliance process to be managed using a multi-layered approach, with transaction monitoring capable of delivering a 24/7, real time, three dimensional picture of client accounts, and any single transaction capable of being de-constructed and analyzed against other historical data to establish a pattern of bona-fides. Anything less will be culpable!
THOMSON REUTERS ACCELUS™

Thomson Reuters Governance, Risk & Compliance (GRC) business unit provides comprehensive solutions that connect our customers’ business to the ever-changing regulatory environment. GRC serves audit, compliance, finance, legal, and risk professionals in financial services, law firms, insurance, and other industries impacted by regulatory change.

The Accelus suite of products provides powerful tools and information that enable proactive insights, dynamic connections, and informed choices that drive overall business performance. Accelus is the combination of the market-leading solutions provided by the heritage businesses of Complinet, IntegraScreen™, Northland Solutions, Oden®, Paisley®, West’s Capitol Watch®, Westlaw® Business, Westlaw Compliance Advisor®, World-Check® and Avanon®.

For more information, visit accelus.thomsonreuters.com