Unweaving the Anti Money Laundering and Counter Terrorist Financing System: Complexity, Simplicity and Paradox Transcript

Date: Thursday, 19 January 2012 - 6:00PM

Location: Barnard's Inn Hall

19 January 2012

Unweaving the Anti Money Laundering and Counter Terrorist Financing System: Complexity, Simplicity and Paradox

Dr Dionysios S Demetis

Welcome.

Before I begin, I would like to thank Gresham College for hosting this event, as well as all of you for being here.

This talk is largely based on my book where I analyse the multiplicity of technology-based influences on the domain of anti-money laundering, and where I develop a systems theoretical approach for the deconstruction of the anti-money laundering domain. The work itself was triggered by a deep interest in Anti-Money Laundering, Information Systems, and Systems Theory. What always seemed to be missing - in my view - was a coherent theoretical framework under which different researchers dealing with AML could unite (on researching and describing the fascinating complexities of anti-money laundering).

In my talk, I will be discussing about some fundamental principles of the broader Anti-Money Laundering domain as well as that of Counter-Terrorist Financing, challenges relating to Transaction Monitoring Systems for dealing with these domains, and I will finish the talk with some reflections on the risk-based approach.

I realise that there are people in the room who have never heard anything about Money Laundering before (or Anti), so let me break it down briefly:

Individuals and/or organisations engage in criminal activity that ranges from drug & human trafficking, extortion, kidnap for ransom, theft, fraud, and the list goes on and on...When they do engage in such activities, they generate profits. Money laundering is essentially all about concealing and masking the origin of funds, placing such funds and integrating them into the legitimate financial system, so that multiple benefits that stem from their use can be enjoyed.

To counter the dynamics of ML, a series of 'international' initiatives have been created. The United Nations, the European Union, the Basel Committee on Banking Supervision, the IMF, have all weighed in with Conventions, Directives, Principles, Technical Assessments and Guidelines. More importantly, the G-8 endorsed Financial Action Task Force (FATF), the key institution behind AML/CFT efforts has introduced 40 recommendations on AML (and an extra 9 special recommendations for countering terrorist financing).

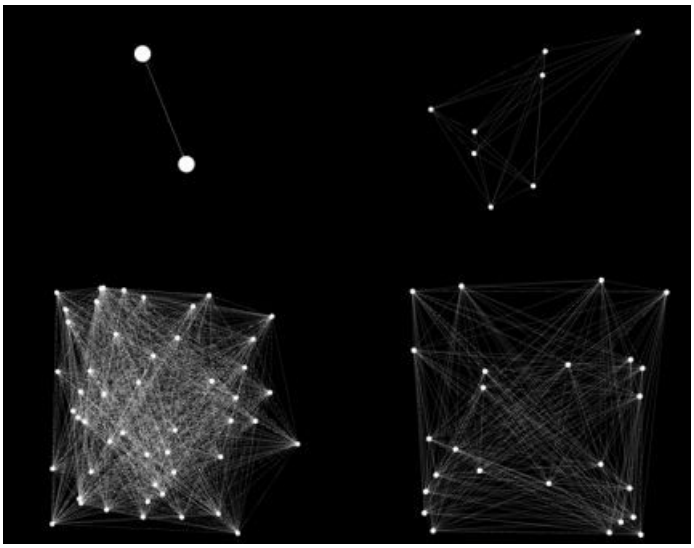
In order to be compliant to such regulatory provisions that gradually trickle down and form into national legislation, financial institutions must deploy a series of monitoring controls & practices. These include Know Your Customer (or KYC) principles, exercising Due Diligence or ECDD, monitoring sanction lists for individuals that are designated as terrorists, monitoring politically exposed persons, etc. But perhaps more importantly, they engage into the continuous monitoring of transaction data. By doing so, they attempt to determine whether your transactions exhibit any signs for money laundering behaviour. And this is where the fun begins. If, a member of staff or a software-generated alert, leads to a strong suspicion that money laundering could be taking place, then a Suspicious Activity Report is sent by the Money Laundering Reporting Officer to a national agency that is known as a Financial Intelligence Unit (or FIU for short). Financial Intelligence Units are then responsible for the aggregation and analysis of all the Suspicious Transaction Reports submitted to them by different institutions in a country. In the event that a case involves multiple jurisdictions, then FIUs from different countries are supposed to communicate with each other for tracking down laundered funds. And while cooperation is important, there are circumstances that render it problematic. 20 years after the constitution of the Financial Action Task Force, the global fight on anti-money laundering and counter-terrorist financing is anything but global.

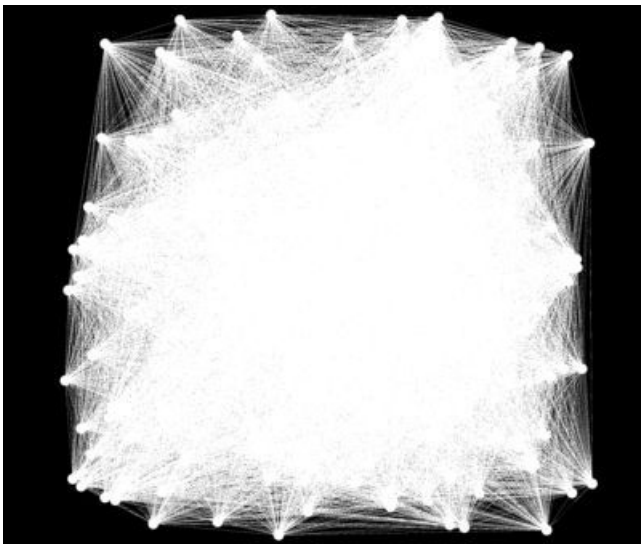
An analysis on data from all nation states recognised by the UN, reveals that there is a significant number of countries that haven't got any Financial Intelligence Unit at all. Other countries do not adequately report on their activities, and many more are not even part of the Egmont Group (the group that joins FIUs together). But even in those cases where Financial Intelligence Units have been established, one can witness a great deal of variation in their reporting structures, while a few lack the capacity to carry out work for analysing multiple reporting sources of ML. Quite simply, if they've got Bank A reporting Person X as a suspect for money laundering and then Insurance company B reports that same person, there is difficulty in putting the two together.

When cases involve multiple jurisdictions where different Financial Intelligence Units need to cooperate with each other for the exchange of information, then it has become standard practice for FIUs to negotiate and sign Memoranda of Understanding for the exchange of information that would lead to successful money laundering investigations, prosecutions, and confiscation of assets. It sounds simple enough that FIUs would and should cooperate but a remarkable complexity emerges out of it.

A visual representation is the best way to see how this complexity evolves when more Financial Intelligence Units need to sign MoUs between them. Each link represents one MoUs that need to be signed for the exchange of

such information. In fact, if all the countries in the world did have operational FIUs - which is not currently the case - and continued to engage in this process, then this is how the whole thing would look like.





But perhaps, a brief informal incident highlights this part of the complex AML system better. Last year, I was chairing a panel session at Cambridge University for the International Symposium on Economic Crime. After the panel and over drinks, I was having a discussion with a Judge who suddenly asked me: 'Do you know why criminals will always be one step ahead?'

So, when I complied with the rhetorical request and asked why, the Judge retorted with a lovely quote and said:

> "Because criminals don't have to sign MoUs"

Taking this line of thinking one step further, it really isn't about the MoUs alone; this type of complexity is propagating across different applications and domains; it characterises the broader entropy of the legal system, a system that attempts to define the distinctions between legal/non-legal. And in doing so, it creates a paradox.

According to famous sociologist and systems theorist Niklas Luhmann, the distinction between legal/non-legal that serves as the code of the system of law {i.e. its systemic identity} has considerable systemic implications because "…while the distinction between legal and illegal can be maintained for individual coding, the legal system as a unity can never decide the basis of what is legal or illegal. It can never apply the code to itself as a system. There is no foundational value establishing what is legal or illegal, only operations." This creates a unique self-reference that is always underpinned by a paradox: "this enables the legal system to operate legally (!) by declaring that something is legal or against the law"

But is it the legal system that 'defines' (anti-) money laundering? What other systems are distorting and re-shaping the legislative designations by infiltrating the heart of any distinctions being used (as in the case of AML, the distinction between suspicious/non-suspicious)?

One thing is certain - that the complexity (and expansion) of the legislative provisions is not to be underestimated. The sheer number of entities that are obliged to exercise vigilance and report suspicious behaviour for money laundering has expanded dramatically. Now over 50 distinct institutional-roles report SARs besides banks. This includes Accountants, Building Societies, Exchanges Bureaux, Insurance companies, money

transmitters, solicitors, etc.

While the vast majority of Suspicious Activity Reports comes from the banking sector, there is increasing reporting from other entities as well. According to the 2011 Annual Report from the Serious and Organised Crime Agency (or SOCA) - the UK FIU, a little more than 192,000 suspicious activity reports have been submitted by banks, corresponding to about 83% of the reporting activity, while a collective 18% amounting to about 30,000 STRs comes from other major reporting entities [note: these figures do not include very low volume reporters of suspicious activity like Securities, Auction Houses, etc]. While the central role of banks in the broader financial system justifies this difference, it didn't use to be like that. A few years ago, bank-generated SARs would account for almost 98% of all reporting activity. This demonstrates that new reporting entities are coming into the game, and that money laundering activities and exploiting entities that are peripheral to the core of the banking sector.

But there is a more general point to be made here.

Year after year, and for the best part of a decade, the number of suspicious transaction reports received by the UK FIU has been increasing. A similar increase has been experienced by most Financial Intelligence Units around the world. The US FIU has experienced a similar trend. This general increase could be interpreted as leading to more cases through the extraction of useful intelligence, or - alternatively - as constituting white noise. Even though there are other reasons that have contributed to the increase of SARs like the increasing number of reporting entities, continuous training on AML that has raised the bar of awareness and the propensity of staff to report suspicious transactions, there is indeed another very important reason behind this increase, and one with a fabric of fascinating consequences. And that one is…Technology.

In particular, transaction monitoring software that 'attempts to simulate money laundering behaviour' by using sequences of transacting patters, common money laundering typologies, and so on.' I find this type of technology fascinating as it abstracts the expectations of how money launderers would transact, and encapsulates those in a series of algorithmic queries. In my book, I have made the case that a whole spectrum of different types of information systems come to influence the basis in which money laundering suspicion becomes constructed. These include: Case Management Systems, different communication systems, intranets, customer database management systems, electronic updates systems, and naturally, transaction monitoring systems.

But when it comes to transaction monitoring, three interlinked aspects come out. First of all, there is a lot of raw transaction data that one has to manipulate in order to 'find' suspicious cases. Secondly, we do our best to come up with algorithms, patterns, queries, thresholds, and so on, techniques that will 'model' the behaviour of ML. And finally, (and more importantly), ML analysts are forced clear the mess every day; the mess created from the many suspicious cases generated by Transaction Monitoring Systems.

Enter the Concept of the True Positive Rate (or the TPR), calculated as the ratio of: the technology-generated reports that are found truly suspicious after diligent manual analysis from staff TO the total number of computer generated alerts. So as an example, if the transaction monitoring system generates 100 suspicious cases and only 10 of them are found to be truly suspicious after manual analysis, then the TPR is 10%.

At Syntax we have been running a survey for some time now on the type of technology being used, the effectiveness of AML-technology, the True Positive Rate (TPR) of their software, what they think of regulators-and-if they've helped them at all in the modelling of ML behaviour, and finally how many queries they actually use to profile Money Laundering Behaviour.

82% of financial institutions have bought a transaction monitoring technology on AML from a software vendor, 9% developed it in-house, and even more interestingly, another 9% had more than one transaction monitoring applications.

When asked 'what they thought of the operations of the AML/CFT software of their financial institution', 18 per cent indicated that the whole project was a disaster, another 27% said that they had a very large number of false positives, … a 36% said that they had customised the software and it has been rather successful but still far off from working properly, and only 18% claimed that they couldn't be happier.

But what constitutes a successful story can carry different interpretations. This is revealed when asked about their True Positive Rate. A 30% responded that their TPR was between 0.1-1%, with an extra 10% having a rate of less than 0.1%. Then, we have rates between 1-5% with a total of 20%, and a remaining 40% having a TPR above 8% but mostly limited to an upper threshold of about 10%. An average bank was spending approximately $350,000 for 5 analysts, just to examine false cases that were generated by the software. $350,000 per year!

Then we asked what was the case when regulators came in for an Information Systems audit of the AML solution. In 30% of the cases, the regulators were perceived as ignorant and having no mechanism whatsoever of evaluating AML-technology performance. In another 40% of cases, regulators were perceived as understanding but having done nothing practical to help, and finally, another 30% are perceived as helpful and provide active advice.

But every monitoring technology is based on queries, rules that attempt to simulate ML behaviour and connect together characteristics and parameters.

This is basically the DNA of modelling suspicious behaviour for money laundering. And while vendors usually provide plenty of predefined rules, we asked financial institutions to tell us how many they were actually using? Here answers were as varied as you can possibly imagine, with some people replying that they used 5 rules to simulate ML-behaviour and others replying 20, 48, even 180, etc. A whole ecosystem of responses indicated so many different approaches, and these made only one thing clear.

That "When a lot of different remedies are suggested for a disease, that means the disease can't be cured", as famous Novelist (& Doctor), Anton Checkov wrote in his last comedy play, 'The Cherry Orchard'.

Countering Terrorist Financing?

Speaking of diseases, there is another resilient one by the name of…Terrorism. Of course, its semantics do depend considerably on the political influences exerted to it. But by stepping-up the monitoring efforts on counter-terrorism, a number of unintended consequences have emerged. False positives are present here as well, and two wonderful examples can be found in the United States no-fly list.

Sister Glenn Anne McPhee is one of them. Not only was she a nun and the head of Catholic Education in the US - but as Wired and many other sources reported, she was also a designated terrorist for 9 months. Despite her numerous complaints to get off the no-fly list, and dozens of missed flights, she couldn't - until some high-level political contacts assisted in the process. The false positives backlog at that time had a 13 month wait.

Another one that apparently exhibited even more suspicious behaviour was Alicia Thomas, a 6-year Old girl from Ohio that was placed on the terror watch list, causing airport havoc whenever her family would fly. But how would a 6-year old end up in the terrorist watch list? When her father was asked by FOX news reporter 'what could she have possibly done?", he responded with a sense of humour… He said: "Well, she did threaten her sister once, but I didn't think this would become a Homeland Security trigger." Such are the troubles of false positives.

Since 9/11, different initiatives have emerged, but one that stands out is the introduction of the 9 special recommendations on counter-terrorist financing from the Financial Action Task Force. In my book, I used a rather provocative heading for the section on counter-terrorist financing and called it a farce. Retrospectively, I was right. Even so, it was not within my intentions to scathingly dismiss CFT efforts, but to contextualise their behavioural monitoring problems.

As a phenomenon, terrorist financing is considerably different to money laundering. This difference lies in the nature of the phenomenon itself, as well as the amount of money required to launch a terrorist attack. For example, the attacks on the London underground cost an estimated £8,000 according to the Official Report submitted to the House of Commons. Also, the9/11 attacks cost between $400,000 and $500,000 to execute according to the 9/11Commission. These figures make one wonder whether the mobilisation of the global financial system is well worth the trouble when tackling terrorist financing.

According to Parkman and Peeling, "those sums spent by active terrorist cells on the preparations for a conventional terrorist attack are typically so small as to be mere droplets in the ocean of daily financial transactions". This highlights the behavioural modelling problem further.

An even more alarming aspect is that the FATF itself seems to agree, since it states the following: "It should be acknowledged as well that financial institutions will probably be unable to detect terrorist financing as such. Indeed, the only time that financial institutions might clearly identify terrorist financing as distinct from other criminal misuse of the financial system is when a known terrorist or terrorist organisation has opened an account".

This quotation has been extracted from within the guidance notes for the detection of TF by financial institutions. - hopefully one spots the irony here.

With the exception of the almost 900 sanction lists where institutions have to engage in a check-and-match process to make sure that they do not facilitate the transactions of any listed terrorist individuals or groups, the automated manipulation of transactions for detecting terrorist financing - is next to impossible in its behavioural sense. And even in the check-and-match process, challenges remain on their implementation at many different levels (linguistic issues, duplication of the lists where effort is required to consolidate, etc). But the monitoring of terrorist financing activity through transaction monitoring raises some other, more controversial issues.

For some institutions, filtering for terrorist financing appears to resort to discriminatory practices that often touch upon sensitive issues of race/nationality and religion, resulting in the phenomenon of 'algorithmic racism' … the phenomenon where personal and sensitive indicators are embedded in algorithmic representations for projecting a probability for terrorist financing. These associations effectively encapsulate terrorist suspicion algorithmically.

This raises another general issue on the data privacy aspects of handling transaction data for monitoring purposes. How individuals are profiled for either money laundering or terrorist financing and what legal rights are transferred to database entries constitutes an emerging issue. In the UK, the report of the Information Commissioner has highlighted a number of important aspects, and the EU is also currently focusing on this issue. Few countries appear to be raising an eyebrow on this matter.

Further on, on countering terrorist financing, a number of aspects are troubling: For example, what is the possibility of a known terrorist or terrorist organisation opening an account instead of having one of their non-listed associates do it for them? - the lists are public anyway. Why not utilise a number of underground Hawala-type methods readily available for moving money around? Thirdly, how could feedback be integrated in such a way that it would support counter-terrorist financing efforts?

One thing that appears to be working is the confidential briefings of Compliance Officers by the National Terrorist FIU of the Scotland Yard, under the Official Secrets Act. Very few countries are engaging in this process and the feedback that I've got from different MLROs is that this has been considerably more helpful and fruitful.

Another interesting aspect to note comes from analysis of more than 30 years of terrorist-related attacks data that I carried out for the purposes of my book. From analysing that data, it became evident that 1400 terrorist organisations have been (and most still are) in existence. More than 12,200 terrorist attacks were recorded in that time frame. And amongst those attacks, 169 different nationalities participated overall, a fact that demonstrates that there is considerable geographical spread over those who are involved in terrorism (this of course depends on the definition of terrorism, another vague construct). But, this geographical spread is in stark contrast to what organisations and countries are targeted for TF. This 'selectivity' - so to speak, finds an example at the OFAC blocked funds, targeting just 8 'terrorist organisations', and with 98 per cent of all block funds corresponding to just 2 of the 8 organisations (namely Al-Qaida and Hamas). The very fact that only $2648 has been confiscated for the financing of the Taliban according to the 2007 Terrorist Assets Report makes a rather strong statement on how 'efficient' the fight against terrorist financing has become. In subsequent reports, the figure has been omitted altogether.

Of course, high-level institutional endorsement of the subject matter of CTF usually prevails over the practical consequences of these difficulties.

The Risk Based Approach

One of the most important evolutions in handling anti-money laundering has been the introduction of the risk-based approach. In the book, I have dedicated an entire chapter in its analysis and in the circumstances that would guarantee its proper implementation. Here, I will attempt to distill only some of the risk-related concepts and describe how they come to affect AML efforts. But before considering risk in the context of AML, it is important first to reflect on both the nature of risk itself and the way it is observed.

Riskis an important concept that is used in the vast majority of financial and other institutions; it is a concept that has influenced much of the handling and management of our modern institutions. But behind the concept of risk there is a widespread misunderstanding, starting with a failure to capture the concept of singularity. A singularity is a unique condition that we cannot recognise as unique within risk. The world is full of singularities.

Even in those disciplines where measurement, risk, and forecast are weaved into each other, singularities dominate and extrude difficulties. When Professor Peter Kennedy published a book on Econometrics with MIT Press, in the prologue of the book, he used an example that made many things clear. In that example, it was stated that:

"to find something meaningful in all that data for forecasting purposes must be so plainly impossible that there will always be endless scope for well-paid advice on how to do it". In other words, accept the inevitability of the future and the effects of singularities. Yet, despite the ambiguities, we seem to be able to consistently ignore the singularities and even claim that risk can be neatly calculated as the product of the probability of an event occurring, times its impact.

Effectively, the product of two entities that are both unknown. Nonsense to put it differently. All the risk-based techniques of the past years in managing the financial system, have not prevented a global financial crisis. In fact, it is more likely that they generated it, by providing a comfortable delusional cushion upon which the excessive risk appetites rested; and with them, the beliefs that we have such a firm handle on uncertainty go on and on. But they cannot account for the singularities. Risk is systemic. It is intrinsic in the systems we use, develop, institutionalise and propagate.

As an entity, risk is both subtle and elusive. Any representation of risk, and hence any attempt to break up risk into sub-categories, carries the initial risk-components unaltered, as in the case of this painting (La clef des champs), from Rene Magritte. As with the shards of the broken glass that carry their original function, risk can be broken down to subsystems that never quite lose their systemic-risk-character.

Thus uncertainty cannot easily be broken down into categories of risk, and even when this is attempted, as in the risk-based approach to AML, the uncertainty is merely transferred to these categories, but without losing any of its essence. All that happens is that risk gains a series of adjectives that incorporate their own distinctions and differences: financial risk, legal risk, structural risk, project risk, process risk, technical risk, and the like; all 'residual categories', comfortable handles that open to the door to the delusion of certainty.

Different ages have had different approaches to uncertainty; different social, cultural, organisational and technological structures, each delivering different notions of risk, different categories of risk, and different risk assessments.

But with the concepts of 'risk' and 'risk management' infiltrating every modern socio-economic and political institution, it is hardly any surprise that some type of risk-based approach was introduced for dealing with anti-money laundering. The EU's 3rd AML Directive have simply put this into some perspective, albeit a vague one that created a series of implementation problems.

Even the semantics of it are non-sensical. It must be made clear that there is a general failure in the risk-based approach to accept this situation. There can be no such thing as a non-risk-based approach! The word 'approach' itself necessarily includes risk.

The word 'approach' effectively demarcates an immediate need to cut down on the complexity in uncertainty, and as Luhmann remarks, 'complexity in this sense, means being forced to select; being forced to select means contingency; and contingency means risk' .

According to Luhmann, the human approach to risk carries an important function: 'since Bacon, Locke, and Vico, confidence in the feasibility of generating circumstances has grown; to a large extent it has been assumed that knowledge and feasibility correlate. This pretension corrects itself to a certain degree with the concept of risk, as it does in other ways with the newly invented probabilistic calculation. Both concepts appear to be able to guarantee that even if things do go wrong, one could have acted correctly'.

Anti-money laundering certainly belongs to a type of system where risk is systemic, in the sense that there is an attempt to control both the interactions and communications for the purpose of improving both the AML system itself, and also the outcomes of its interactions with other systems (i.e. legal system) in order to reach successful prosecution of ML cases and consequently confiscate illegally acquired assets.

And one of the prevalent distinctions being used for risk is between high-risk and low-risk categories for money laundering. This is a nice and comfortable 'grey area', a grey area for all sorts of different categories.

Many analysts, and indeed the FATF itself, recommend a delineation into 'high- and low-risk' products or services. For instance, products and services such as private banking, correspondent banking, wire transfers, e-banking, use of credit cards etc. are typical examples of perceived high-risk for ML. These can be then categorised in a potential product/risk matrix in order to examine the volume of activity, to monitor the potential risks that are faced within each institution, and to demonstrate a prudent methodological structure for compliance purposes. Similarly, high-risk customers are also considered for which typical risk-scoring systems can be created; money transmitters, cheque cashiers, security brokers and dealers, property dealers, professional and consulting firms etc. The list goes on and on. According to the risk-based approach, exporters, importers, and all cash intensive businesses (retail, restaurants, second hand car dealerships, offshore corporations, banks in secrecy havens, as well as non-profit organisations like charities) are also increasingly being manipulated by launderers. Thus this group of high-risk customers should head the list of those being reported.

But the fact that we can designate such categories does not necessarily mean that such categories can automatically incorporate the totality of a single category (say high-risk customers). This is the foundational error of the risk-based approach: there is nothing intrinsic in any of these categories that can force them into being designated as high-risk for money laundering. Any category can, at the same time, be both part of the high-risk and low-risk assessment process.

For example, let us take a cash intensive business like a retail store as our category. But once one defines that to be a category then it is inevitable that varieties within the same category (namely different retail stores), risk-subsystems in themselves, will be part of both high- and low-risk assessment processes regarding money laundering.

Any category itself is therefore a risk-based hybrid! When the category opens itself up for classification as qualitatively either 'high' or 'low' risk (before being assigned a probability) it cannot resist being simultaneously part of both 'high' and 'low' risk areas. This simultaneity owes its nature to the malleable nature of risk itself and the considerable difficulty that is placed in its abstract nature.

Given that any category can be portrayed as a risk-based hybrid of both high- and low- Money laundering and Terrorist Financing risks, the current way of classifying ML-risks is simplistic. It is an anachronism based on the fundamental misconception that risk becomes diffused once broken down into its subsystems (risk-categories), a misconception that cannot withstand proper analytical scrutiny and one that does not recognise the gravity of

the problem of the reflexivity and re-genesis of risk (the fact that risk re-generates itself).

To deal with the risk-based approach, we need context-sensitive data that will act as 2nd order proxies for determining risk-levels of risk-categories. We need mechanisms that will treat Anti-Money Laundering as a system, and attempt to figure out what information from its environment can be used for enhancing behavioural modelling. This does not have to come from outside of the organisation. Data from the marketing department, or even the sales department can be used to enhance monitoring profiles.

In other words, we need to have a way where different proxies for monitoring parameters for money laundering behaviour can be synthesised between them in order to designate this difference between high/low-risk categories. But in this area of application, there is no silver bullet.

This becomes evident in the concept of risk-sensitivity, a concept that is even more elusive than risk itself (!) and used throughout the 3rd EU Directive and various other guidelines. How does the concept of risk-sensitivity stand up, when in effect it is like asking 'how risky risk is'? How much of this terminology has any scientific basis, and how much is it wishful thinking?

For practitioners that have to deal with the modeling of money laundering behaviour or the technological integration of queries that simulate transacting patterns that could potentially lead to suspicious transactions, this was always assumed to a large extent. They were aware of the fact that any course of action would open up possibilities whilst restricting others.

For Central bankers or supervisory authorities that had to audit the risk-based approach, things became also confusing. They were asking: "How are we supposed to audit the financial institution's interpretation of AML/CTF risks? - what is the yardstick?" If we abandon the 'one-size fits all' approach then how many 'malfunctions' are we prepared to take? For governments on the other hand, the risk-based approach opened an amazing opportunity due to the flexibility of risk-interpretation itself.

As one official from a Central Bank told me (from another EU-member state), "we would be very interested to see what other governments are doing with the risk-based approach on ML/TF and how they are integrating it…we would like to call it… regulatory arbitrage!" Touché!

Governments come under the same 'roof' to create a series of legislative initiatives in order to fight ML/TF but, at the same time, they remain concerned that too stringent legislative provisions could deprive them of business. There are always unintended consequences. The introduction of the Foreign Assets Controls Tax Act (or FATCA) is one such example. My view is that it is not within the US-interests for FATCA to go through. Empirical data to support this assertion can already be found in Switzerland where there is a 12-month waiting list in the Consulate, from US citizens who want to abandon their citizenship. From the individuals being affected, unintended consequences can be found in institutions affected. In the UK, the Financial Times reported that big banks were considering a move out of London claiming that 'HSBC, Barclays and Standard Chartered have given clear signals that they would be willing to move their headquarters overseas if the regulatory onslaught on the UK financial industry intensified'. Now, that's a risk!

What will the future hold for AML/CTF a few years down the line? International cooperation will have gained (hopefully) a bit of momentum in the critical issues of communication and standardisation, some greater clarity will be sought (methodologically) for the sound implementation, audit, and integration of the risk-based approach, and just perhaps, some of the things that we take for granted will be re-considered as we will be moving into another AML/CTF compliance cycle.