THE GUERNSEY SOCIETY OF CHARTERED AND CERTIFIED ACCOUNTANTS

5 JUNE 2014

PRESENTATION BY SAMANTHA J SHEEN

HEAD OF THE FINANCIAL CRIME & AUTHORISATIONS DIVISION ("FC&A Division")

Introduction

Good Day Everyone

As you've read from the flier about this luncheon today, the focus of my presentation will be on financial crime risks relevant to international finance centres, and in particular, a couple that may be of interest to the Moneyval assessors who will be visiting the Bailiwick in the first week of October this year.

Overview – Financial Crime Team

First though, let me tell you a little bit about my team. The financial crime team in the FC&A Division comprises 7 members of staff who are wholly devoted to the supervision of all regulated and registered businesses in relation to financial crime. The team is responsible not only for undertaking supervisory activities, such as on-site visits, thematic desk-based reviews and statistical trend analysis, but is also responsible for policy review and development, public outreach, industry awareness and education.

As part of its policy responsibilities, the team has been closely monitoring the activities and assessment reports being generated by international assessment bodies such as Moneyval, and international standard setters, such as the Financial Action Task Force, or FATF. The team also liaises closely with fellow international finance centres who have been assessed, and representatives from those jurisdictions who have taken part in some of the assessments conducted in the last 2 years.

Perceptions of International Finance Centres

It's clear from the information we have obtained that there continues to be a perception, and unfortunately a negative one, that centres such as ours are

regulated to a minimal standard and that business is conducted for maximum commercial gain with little regard for any financial crime risks to which those businesses may be exposed.

Just last week, I was part of a panel at a European AML conference. I cannot tell you the number of times I had to listen to how the Channel Islands was a "tax haven" and that we undertook business here with little concern for its legality.

Now, I suspect this is an audience of people who do not need convincing that these sorts of statements are just plain wrong. In fact, I suspect that a number of you would say, especially if you are compliance officers, that the regulatory burden in relation to AML/CFT here can sometimes seem hard-going.

Many other international finance centres join us in sharing the challenge of evidencing to other jurisdictions that our industries are aware of and take seriously their obligations towards the detection, prevention and mitigation of financial crime.

As I mentioned earlier, my team has been monitoring developments at the international level in order to identify what specific perceptions around ML/TF risks are being more commonly attributed to centres such as our own.

I don't propose to go through all of these risks, and I will explain why nearer the end of the presentation. But here are what I think are the two most significant ones.

Business Risk Assessments

First off, business risk assessments. There is a concern that business risk assessments are not done in a meaningful way. So what does that mean? Well, international assessors appear to be looking to businesses and asking how that assessment informs their risk appetite. In other words, having undertaken the assessment, where does the business pitch the level of risk it thinks, based on its size, nature and complexity, it can manage and mitigate in relation to the possible financial crime risk exposure that may be associated with its products, services and customers.

Now this might seem a bit of a woolly concept, but let me try to explain further why this seems to be a cause for concern.

If you were at my GACO presentation in January, you might recall me using the terms accumulation of risk and confluence of risk. The accumulation concept is fairly straight forward – it's a 1+1+1 = 3 exercise.

Confluence is a slightly different concept. The idea here is that sometimes the cumulative effect of 1+1+1 results in something greater than 3, for risk purposes.

Unless a business is alive to both these concepts it may underestimate or miscalculate both the nature of controls it requires and amount of resources needed to effectively mitigate potential financial crime risks.

Stay with me, while I explain this further. There is a particular concern that international finance centres predominantly operate on a non face-to-face basis with their customers. You will know from our Handbooks that simply having a non face-to-face relationship is not a factor in and of itself, to rate a relationship high risk. The Regulations and Handbooks require that certain controls be put in place in order to mitigate the risks that could arise. Using copy documentation provided by a suitable certifier, is one example of such a control.

Typically, what most businesses will do is work their way through a customer's profile, looking at jurisdiction, nature and purpose of the business, whether the customer is or is associated with a PEP, the complexity of their structure, etc. If each of these characteristics is assessed as low risk, that's the rating assigned.

In some circles, there appears to be increasing concern that businesses are not looking at risk "in the round", when it comes to customers and the knock on effect it has on the effectiveness of the measures they adopt in order to mitigate financial crime risks.

Let me give you an example used in one assessment we reviewed. Imagine you have a new customer who undertakes its business from a jurisdiction who is otherwise not listed in one of the Commission's Business from Sensitive Sources Instructions. The customer comes to the business via a business introduction. What is meant by that is that the arrangement has come by way of a referral from another party, say a law firm, but not the sort of formal Introducer

Arrangements as are described in our Regulations and Handbooks. The business therefore does not meet the customer initially in person in order to establish the relationship, relying on certified documentation verifying the identity of the customer.

First off, let's consider the concept of accumulation of risk. In this scenario, the business has not met the customer or its ultimate beneficial owners. It is going to rely on someone to have actually met the customer and then certify that a photocopy of a passport, for example, really is the true likeness of the customer. The customer's structure might entail a trust or private corporate entities for which there is little on public record as to their commercial use and the activities so again reliance may need to be placed on copy documentation produced by a third party. Now add to the additional risk factors that may be posed by the jurisdiction, the products themselves or the delivery channels.

The accumulation of risks concept suggest that perhaps when, looking at each of these risks, a risk rating for each of them could be assigned and then the sum total should lead to an appropriate risk rating assigned that will further inform the level customer due diligence and ongoing monitoring required of the relationship.

But here's where the concept of confluence becomes important. Think of the scenario I have just described. Consider each of the characteristics as a pane of glass – the kind of glass people put on their front door – a bit frosted so that they can see that someone is there on their front porch. That's the non-face to face part. You are reliant on external parties to verify the identity of the customer. Limited access to public information may also limited the clarity you are able to obtain around the customer's activities. This adds another pane of frosted glass to the original window. Now add a third pane for all of the other factors I've mentioned.

The overall effect of this is to increasing obscure or reduce the transparency of the window, so that whereas before you could make out who was at your front door you now can only make out a silhouette of who is standing on your doorstep. When each pane is considered separately, they are fairly transparent. But when the effect or interaction resulting from having the three panes in place is considered, the confluent effect compounds the lack of transparency. This

means that undertaking a 1+1+1 exercise when considering risk factors can actually cause a business to mis-rate or under-rate the overall risk presented by a given relationship.

It's these two concepts that some assessors believe may be prevalent in the businesses operating in jurisdictions such as ours. The presumption is – how can you properly mitigate financial crime risks with your policies, procedures and controls if you don't really understand and properly take account of the overall risk that your customers could pose from a financial crime perspective?

And this concept also applies with respect to a firm's business risk assessment. How can you properly design, review and modify your compliance arrangements if you have not considered how the risks you've identified could interact and possibly escalate the level of financial crime risk exposure for your business?

All fairly theoretical? Not quite. In 2013, MONEYVAL undertook an assessment of the Cyprus banking sector. Now, the reasons for the visit and the nature of the banking sector, along with the degree of regulation of the accountancy sector, are all distinguishing factors, but they don't detract from the point I am about to make. Because this assessment provides a very good example of how the confluence of risk actually happens and how it can compromise the utility of a business risk assessment, if risk is not looked at in the round.

One of the findings from this assessment was that a number of the banks were using automated systems to undertake customer monitoring. It so happens that a number of these banks had customer bases that comprised of a number of individuals from Russia and the Ukraine.

The way in which the systems were calibrated was such that as a result of the customer's risk characteristics, the systems generated a large number of automated alerts. The problem? There weren't enough staff to actually investigate the alerts, so many of them were not looked into.

These banks had undertaken business risk assessments and from that designed their AML compliance arrangements. Now Cyprus, like Guernsey, does a lot of non-face to face business. They were relying on certified documentation and their customers involved complex structures.

When these banks undertook their business risk assessments, they did not take into account how those characteristics might raise the level of risk for their businesses and in turn the amount of resources they would need in order to have appropriate and effective controls to mitigate those risks.

So, in North American parlance, they "low balled" their assessment of what they needed to have in place. Imagine you're the compliance staff. Your monitoring procedure requires that you check any alerts on your automated system within 48 hours. But wait, you can't do this quickly because no one at your business has actually met this customer or the beneficial owners. You are relying on a referee, who provided you with the certified documents but maybe they themselves were not the certifiers. You don't have a formal Introducer Arrangement in place so they have no obligation to keep that CDD up to date and to provide to you upon request and without delay.

The referee or certifier probably has not contacted you to tell you if any adverse information has subsequently come up about the customer.

You can't quickly locate any publically available information about the customer's corporate structure, because it's incorporated in a jurisdiction where the corporate register is not accessible to you.

So how are you going to comply with a 48 hour deadline for all of these alerts? There are only so many hours in a day, you still have your own BAU to compete and you are not going to get senior management buy in to hire you some more compliance staff at the last minute.

This is how confluence of risks can manifest themselves to compromise the appropriateness and effectiveness of a business' compliance arrangements. And these are not unpredictable or unpreventable risks. But having not been looked at in the round when the risks to the business and the controls that would be needed, were being assessed.

That then brings us full circle to risk appetite. If you haven't properly assessed the risks to your business, the impact of their accumulation or confluence, you are at risk of implementing inappropriate and ineffective compliance arrangements that do not mitigate the financial crime risks, as intended. An

assessment of risk in the round provides a business with a more realistic idea as to the resources that will be needed for compliance purposes, to mitigate the possible financial crime risks. This then will allow the business to make a commercial decision as to whether it can afford to resource the necessary compliance measures needed to mitigate these risks and if not, at what point will the seesaw swing downward where the degree of risk being assumed cannot be mitigated by the controls measures needed.

Suspicious Activity Reporting ("SAR") and Rejected or Exiting Business

I would now like to quickly move to one last point. This has to do with suspicious activity reporting.

The reporting requirements include not only transactions but also activities. These requirements cover not only activities that take place with existing customers, but also where a business forms a suspicion about a prospective business relationship or occasional transaction, which it subsequently rejects or declines. This requirement also applies where a business exits a business or where a suspicion is formed about the circumstances in which a customer has requested that its account or services be terminated or a corporate structure wound up.

A concern is raised from time to time that businesses in international finance centres are not making SARs in these instances. Concerns have also been raised about the failure of some businesses to maintain an accessible record of rejected business. I can understand these concerns because a prospective customer could attempt to make contact to establish a business relationship with different departments within the same organisation or with its offices in other jurisdictions. Criminals may attempt to again establish a business relationship by allowing a period of time to pass on the assumption that their previous rejected attempts will have been forgotten.

It is in the interests of all of us, particularly given the non face-to-face nature of some of the business undertaken in the Bailiwick, that everyone take steps to protect both their business and the Bailiwick as a whole, by maintaining a referable record of rejected business and that suspicions formed about prospective and exiting relationships are reported promptly.

We will then collate the results and, discuss both these and the other risks identified from our review of international assessments with a working group comprised of representatives from this industry association in late August.

Ladies and Gentleman, those are my comments for this afternoon. Thank-you for listening.