SUMMARY OF THE PRESENTATION TO THE GUERNSEY ASSOCIATION OF COMPLIANCE OFFICERS

FINANCIAL CRIMES SYMPOSIUM

SAMANTHA SHEEN

HEAD OF THE FINANCIAL CRIME & AUTHORISATIONS DIVISION

29 JANUARY 2014

Introduction

The study of financial services risk management often involves the use of case studies and typologies that are not always directly related to the financial services sector. One case study, for example, involves a retrospective risk assessment on the reasons for the sinking of Henry the VIII's favourite war ship, the Mary Rose. What makes this case study relevant is what it teaches about risk assessment, the importance of reviewing such assessments and the escalation of risks where a confluence of factors occurs.

While the individual factors which may have contributed to the sinking of the Mary Rose, when each looked at in isolation from the others, appeared manageable using existing controls, a very different outcome may occur where the risks posed by those factors all came to fruition in or about the same time.

Today I would like to build upon the two ideas that came out of the Mary Rose case study – the importance of reviewing risk assessments and the confluence of risk factors – as they relate to business risk assessments and client risk assessments undertaken by the regulated financial services sector here in the Bailiwick. I will the conclude my talk with some remarks as to what the Commission expects from the regulated sector in terms of applying these two ideas and how financial crime risks are managed and mitigated.

Confluence of Risk Factors – Client Risk Characteristics

So, let me start with the second idea – the confluence of factors. Confluence occurs where factors which often seem unrelated have interdependencies that contribute to a level of risk exposure that is higher than would otherwise be the case when each of those factors is considered in isolation. Another of way of describing this in practice is "risk in the round". When assessing money laundering risks based on a client's risk characteristics, for example, one will not only look at each risk factor individually, but also look at the picture that those factors present collectively in order to determine the possible exposure to which a firm might be exposed.

Looking at risk factors "in the round" requires that the design of a firm's customer due diligence systems and controls allows for this collective consideration to occur. Unfortunately, some firms will endeavour to simplify their client risk assessment process by designing a prescribed check-list style process. The motivation behind this design is so as to ensure that the firm's staff members readily understand what needs to be collected and verified in order to satisfy the regulatory requirements. Although the objective is positive, the unintended consequence of systems designed in this way is

that the more prescribed the process is, the more likely that an individual's perspective is drawn away from actually seeing the cumulative – or real-level of money laundering risk that may be present.

So, by way of example, one client risk characteristic is whether this is to be a face-to-face or non face-to-face relationship. It is generally understood that the latter poses a greater risk than the former. Controls are therefore put in place by firms to mitigate that risk. The nature of those controls may be such that when applied, this results in a low risk rating in respect of the client in question. However, were we to add to this client's risk characteristics the fact that they form part of a more complex corporate structure spread across several different countries, and that the client was being introduced by a reliable introducer, there may be additional challenges posed around the transparency of that client and their activities. Were each of these factors to be assessed in isolation, a rating of low risk could be assigned for this client relationship. However, the confluence of those risk factors could mean that the possible limits in relation to transparency warranted a rating of this relationship as other than low risk, and in turn, the application of different controls to mitigate that risk.

Failing to recognise the effect of confluence can therefore mean that in some instances, a business that should be undertaking enhanced monitoring is not doing so, and as a result of which, may fail to identify changes in that relationship which warrant further scrutiny in a timely manner.

Confluence of Risk Factors – Systems and Control Failures

A particular concern for financial service regulators is whether the level of a firm's money laundering risk exposure has been escalated due to confluence arising from the firm's own systems and controls. This can often occur in the following way.

First, after a period of "good performance" or positive results from periodic checks, the scope or time periods for reviews are often relaxed or attention is instead drawn to other areas of priority. Over time, the nature of the business undertaken by the firm starts to change. This may occur through a gradual increase or change in business derived from existing clients, the departure of long standing compliance and other key relationship staff members or a change in software systems. As a result, the nature and extent of the firm's money laundering risk exposure also starts to change. As time goes on, staff members become less attentive to adhering to these systems and applying the controls. A degree of forgetfulness can set in. Staff members may start to forget what the systems and controls were for and what AML risks they were designed to mitigate. This then leads to instances where staff members start to work around the systems and controls and those "work arounds" start to subtly replace them.

The pace at which this occurs will vary from firm to firm, but it is almost inevitably discovered when a risk event comes to fruition or the regulator conducts an on-site visit, and the firm realises that it has allowed itself to be lulled into a false sense of security about the appropriateness and effectiveness of its systems and controls.

<u>Financial Conduct Authority (FCA) Decision: Standard Bank PLC 22 January 2014</u>

Last week the FCA imposed a financial penalty of approximately £7.6 million on Standard Bank in the UK for failings related to its anti-money laundering policies and procedures over corporate clients

connected to politically exposed persons ("PEPs"). The facts of this case are a useful illustration of the confluence of risk factors and the impact of systems and controls' failures.

Standard Bank had approximately 5,000 clients of which approximately 5% were linked to PEPs. The FCA found a number of other failings relating to the adequacy and effectiveness of the Bank's systems and controls to mitigate money laundering risks associated with PEPs and how these risks were escalated due to the confluence of these failings. The failings of note were as follows:

a) Although some EDD had been undertaken on the clients with links to PEPs, on the majority of the files reviewed, the Bank had failed to follow its own EDD requirements. This meant that some of these clients were not rated a high risk and in turn were not subject to enhanced monitoring.
b) Some client relationships had been mis-rated. This was because staff had, in some cases, assigned risk ratings based solely on the jurisdiction in which the corporate client was incorporated, despite the presence of other clear, high risk characteristics.
c) Although the Bank had subsequently changed its risk classification process, the procedures when put in practice rendered it ineffective. The task of assigning the risk rating was segregated from the task of determining the level of due diligence to be undertaken. As a result, the new system resulted in the corporate clients being correctly classified as high risk due to their links with PEPs, but then no enhanced due diligence was undertaken on them.
d) The FCA found instances where staff undertaking due diligence on the high risk corporate clients had sought and obtained "exemptions" from the compliance team from having to undertaken EDD. The exemptions were sought due to difficulty experienced in obtaining the necessary due diligence from those clients.
e) Although the Bank had automated and manual transaction monitoring in place, it failed to apply its own client assessment review procedures. In some cases, reviews were late by a matter of months, while in other cases, years. The FCA found this failing for approximately 80% of the Bank's overall client base.

The failures identified in the Standard Bank case reflect the subtle creep I described earlier which renders systems and controls ineffective. This case raises concerns in two respects:

First, the failings meant that the Bank could not undertake an effective client risk assessment of these corporate clients. In the absence of obtaining the necessary EDD, the Bank would not have been able to look at the complete risk characteristics of these clients and assess the overall money laundering risk exposure which they might pose. Without being able to look at these risks "in the round", the Bank was unable to truly make an informed judgement as to (1) whether it wished to establish a business relationship with these clients, (2) if so, what the complete risk profile of the client was expected to be in terms of transaction activity and source of funds and wealth and (3) whether enhanced monitoring over and above that required by its EDD procedures was warranted to mitigated the potential associated money laundering risks.

Second, the extent and nature of the failings calls into question the manner in which the Bank was reviewing and assessing its compliance arrangements to verify that they were, and remained, appropriate and effective, given the nature of its business activities and associated money laundering risk exposure. The facts in this case suggest that the Bank had been operating for a

period of time during which the money laundering risks to which it may have been exposed were neither managed nor mitigated against.

Financial Services Authority Decision: EFG Private Bank Limited 28 March 2013

In March 2013 the FSA imposed a financial penalty of approximately £4.2 million on EFG Private Bank Limited ("EFG") in the UK for failing to take reasonable case to establish and maintain effective anti-money laundering systems and controls in relation to clients that were identified by EFG as posing a higher risk of money laundering.

The failures, in some respects, were similar to those in the Standard Bank. However, unlike in that case, the FCA found evidence of instances where EFC had taken on clients despite the presence of adverse information, including allegations of fraud or corruption. The evidence held on these client files failed to demonstrate how EFG's senior management had recognised and assessed these risks before client take-on, despite this being a requirement of its own policies and procedures.

It could be argued that by failing to apply its own procedures, EFG had also adversely affected its on-going monitoring measures. Without knowing why the clients had been taken on, despite these high risk indicators, EFG's staff could not reasonably have been expected to be aware of the specific risks to be monitored and may well have overlooked them were they to arise.

The FCA also found that EFG had failed in a number of instances to obtain information concerning the source of funds and wealth of clients which it had rated as high risk. In one case, for example, EFG had accepted a multi-million pound deposit which it was told by the client related to the sale of overseas property. EFG's compliance department requested a copy of the property sales contract before the funds were accepted. Despite this request, the contract was not provided by the client and the funds were accepted.

Akin to the Standard Bank case, the FCA found large gaps of time in relation to EFG's application of its own monitoring and risk review procedures, particular in relation to PEPs.

Financial Conduct Authority: JLT Speciality Limited 19 December 2013

The final FCA case which illustrates this phenomenon of confluence involved JLT Speciality Limited ("JLT"). In December 2013, the FCA imposed a financial penalty of approximately £1.8 million for failing to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems and controls for countering the risks of bribery and corruption associated with making payments to overseas third parties that helped JLT retain business from overseas clients.

As part of its compliance arrangements, JLT had in place a system known as the "7 alarm bells", which it used to assess and manage the risks of bribery and corruption relating to its overseas introducer arrangement. The system was set up in such a way that if any one of the "bells" or risk factors was present, the proposed introducer arrangements had to be referred to a director for approval. A single bell which amounted to a "sufficient concern" required that referral be made.

The problem with this system was again in how it was applied. First off, the term "sufficient concern", was not defined. This meant that it was left to the staff member dealing with the

arrangement to determine for themselves whether referral was warranted. No guidance had been issued to JLT's staff on what the company considered to constitute a "sufficient concern".

Second, JLT had sought assurance around the system's effectiveness by having it reviewed and assessed against its compliance with the UK bribery legislation. However, the review itself was flawed. While the review verified that the system's requirements allowed for compliance with the legislation, it failed to verify "in the round" whether the system was actually being applied and effectively mitigating bribery and corruption risks around introducer relationships.

Third, the FCA found that JLT failed to conduct adequate CDD before entering into relationships with, or making payments to, overseas introducers. Key to this was JLT's failure to ensure that its CDD procedures verified whether there was a connection between an introducer and the client or an introducer and any public officials. The 7 bells system did not provide any guidance to the staff on how to go about doing this. And although JLT required that a database search be undertaken, the software being used, alone, would not have allowed JLT to comprehensively check whether any connections existed.

Even the limited benefit of the database software was compromised by virtue of how the staff members were undertaking their searches. Although the name of an overseas introducer was checked, the names of the directors or beneficial owners were not consistently checked. There were other failings in relation to how the searches were being undertaken, all which compromised the effectiveness of the CDD procedures and software tool which JLT had put in place.

Even when a connection had been found, there was further evidence that JLT's staff did not conduct any enhanced due diligence to counter the risks of bribery and corruption presented by these higher risk relationships. It turned out that a significant proportion of the overseas introducers either had a direct connection with the client being introduced or there was a connection with a state-owned corporate body or the introducer themselves turned out to be a PEP.

Confluence of Risk and Business Risk Assessments

After considering these cases, how might a business risk assessment be relevant to a firm's awareness of the confluence of risk factors?

A business risk assessment sets the barometer for a firm's risk appetite. And one cannot fully know what that appetite might be unless there is an understanding as to how ML/TF risk exposure "in the round" may occur. The business risk assessment is really the frame from which a firm's policies, procedures, systems and controls are supported.

In order to serve this purpose, the completion of a business risk assessment requires that questions be asked, such as, "How much potential risk exposure can we bear as a business, given the systems and controls we will need to have in place to manage and mitigate those risks?" "How robust are our existing measures and do they have sufficient reliance to effectively manage ML/TF risk exposure variations that may result from changes in business strategy?"

The Moneyval special report on the Cyprus banking sector provides a good illustration of the types of events that can give rise to the confluence of risk, and the importance asking these questions.

One example concerned the banks' reliance upon technology. In theory, the technology allowed for a robust and ongoing monitoring of the banks' client base to ensure that any changes to risk profiles were quickly identified and investigated. This tool seems ideal, except that its application and the support needed to maintain its effectiveness, was not fully realised. As the banks' underlying client composition changed, for various reasons, so too did this result in a marked increase in the number of changes which required investigation. The problem then arose that there were insufficient resources available to actually investigate those changes. This then had a knock-on effect by requiring that staff redirect their efforts from other activities to trying to clear the back-log. And as we all know, when there is a large backlog of reviewing to be done, often the significant matters are overlooked for the sake of clearing it.

This is precisely why it is so crucial that compliance arrangements are reviewed in conjunction with the business risk assessment and that the risks to which the business may be exposed are considered, not just in isolation, but in terms of how their interaction with one another might give rise to an even greater ML/TF risk exposure.

Commission's Expectations

The nature of the non-compliance in the 3 UK cases I have mentioned, from a historical perspective, are not unknown in this jurisdiction. The Commission's approach in such cases has been, and continues to be, that there will be little tolerance for such failings. This is for two reasons:

(a) The failings identified are not only within the control of firms, but is something which they are required to be alive to on an ongoing basis, pursuant to Regulation 15 of the AML/CFT Regulations, a requirement that has been in place since 2007.
(b) Such failings not only expose the business to the risk of its products and services being used to launder the proceeds of crime, but also expose the Bailiwick to adverse reputational risk as an international financial centre.

Conclusion

So, what are the lessons to be learnt from the Mary Rose and the other cases that I have mentioned today? What does the Commission expect when we hear about firms' compliance arrangements?

First, it is recognised that the dynamic nature of business requires that innovation and change form a part of daily business activities. In the Mary Rose case study, changes were happening at a number of stages throughout its life, all of which altered the effectiveness of its original controls.

Firms are expected to review their business risk assessment in a way which evidences their awareness of both prospective and actual changes that have taken place, be it a change in outsourcing provider, products and services or client composition. Firms should be able to explain how they have undertaken their business assessment review, and describe how they have arrived at the decision whether to vary that assessment, or not. The assessments themselves should reflect a consideration of risk "in the round" and whether a possible confluence of risk factors could occur, warranting controls to mitigate the escalated ML/TF risk.

Where there is evidence that change has occurred which could give rise to a change in the factors or risk exposure of those factors considered as part of the business risk assessment, it will not be sufficient for a firm to wait until some pre-determined date in the future to undertake a review.

There should be a demonstrable connection between the business risk assessment and the compliance arrangements of a firm. A review of the policies, procedures, systems and controls should reflect a consideration as to whether changes to the business risk assessment also require that changes be made to those arrangements to ensure that ML/TF risks are mitigated. That review must include an assessment as to the appropriateness and effectiveness of those arrangements, not just in terms of their compliance with the regulatory requirements, but also whether they are understood and applied by the staff required to follow them. Firms should be able to demonstrate the methodology used to undertake this assessment.

A dim view will be taken of firms who fail to comply with their own systems and controls that are designed to mitigate the risks associated with PEPs, other high risk clients, bribery and corruption. Failure to do so means that a firm is working with a blind spot and unable to demonstrate a complete understanding of the risks to which such clients and activities can expose the firm.

A review of client risk assessments relating to PEPs should involve more than a proprietary database search. Firms are expected to undertake that review with reference to the client's existing profile at take-on, expected versus actual transaction activity, and new public information. And of course, a record must be maintained of decisions made as a result of such changes. There should therefore be an active, demonstrable consideration of a PEPs risk profile as against new or additional information.

Finally, firms are encouraged to review the content of staff training to ensure that staff are taught how to undertake client risk assessments, Firms should ensure that their staff understand the importance of looking at risk "in the round" by considering a client's profile on the whole, and not each of its characteristics in isolation of the others. Firms should ensure that their staff understand the risk of the confluence of risk and how this can be mitigated.

As an international finance centre, the Bailiwick has prided itself in countering suggestions that the mere presence of private banking and fiduciary activities warrants a blanket risk rating of them as high risk. Such suggestions have been countered by pointing to the Bailiwick's robust regulatory framework, the diligence of our law enforcement authorities, the supervision undertaken by the Commission and other regulatory agencies and the compliance demonstrated by our regulated sector.

As compliance professionals, you have a critical role to play. We look to you to ensure that your firms understand the importance of applying the requirements which ensures that risk is managed "in the round", treated as an iterative matter and are alive to how a combination of risk factors, can increase the potential ML/TF risk exposure of your firms.