Risk impact is in the eye of the beholder: The difficulties faced by the regulator in an offshore financial centre

Paul Coleman

Received (in revised form) 18th April, 2017

Turks and Caicos Financial Services Commission, Caribbean Place, PO Box 140, Providenciales, Turks and Caicos Islands, BWI
Tel: +1 649 431 4797; E-mail: pjlcoleman@yahoo.co.uk

Paul Coleman *is Director of Compliance for the Turks and Caicos Islands Financial Services Commission (FSC), which he joined in November 2012. His initial appointment was to implement extended coverage of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime in the Turks and Caicos Islands to designated non-financial businesses and professions. In June 2014, Paul's responsibilities were increased to lead the newly formed compliance unit of the FSC with AML/CFT supervisory responsibilities for the broader group of all bank and non-bank financial businesses as well as non-profit organisations. Paul has a distinctive professional background in AML both internationally and in the Turks and Caicos Islands. He has almost 20 years' private sector experience operating throughout the UK and the Caribbean, and in particular the Turks and Caicos Islands, holding positions in retail and international banking as an internal auditor, business development director and money laundering reporting officer. He is now operating in the supervisory discipline for the FSC. Using his wide ranging specialism, Paul has also acted as an expert witness for a number of anti-money laundering legal cases. Paul is a qualified banker, internal auditor and certified advanced AML audit specialist (CAMS-audit).*

Abstract

Protecting the financial integrity and reputation of the financial sector by achieving strong anti-money laundering and combating terrorist financing regimes is a crucial responsibility of the regulator. Conflicting objectives exist between the regulator and the financial institution based upon their assessment, should money laundering occur, of the reputational impact to the country's financial sector and to the financial institution itself. The expectation of the regulator, through rigorous supervision, to uphold the integrity of the financial sector continues to increase. While agreeing with the concept of effective management of money laundering and terrorist financing risks, the financial institution must protect the integrity of the financial system in the context of an environment of demanding cost constraints. This paper considers the impact of centralisation as a cost effective operating model against the increasing demand and expectations for robust regulatory compliance, highlighting the conflicting objectives of both the regulator and the financial institution.

Keywords: offshore financial centre, anti-money laundering (AML) compliance, risk, transaction monitoring, regulator, regulatory fines

Paul Coleman

INTRODUCTION

Regulators and financial institutions typically agree on the importance of compliance with anti-money laundering and combating the financing of terrorism (AML/CFT) legislation. Their viewpoints towards implementation and monitoring are, however, likely to be

Journal of Financial Compliance
Vol. 1, No. 1 2017, pp. 37–45

2398-8053

different. Such differences emanate from conclusions of risk impact drawn from their respective money laundering and terrorist financing (ML/TF) risk assessments.

The differing views and consequences on risk impact become more marked when regulator expectations encounter the management of ML/TF risks by global institutions operating in remote jurisdictions. Conflict results between the regulatory need to maintain the highest standards against the cost objectives of financial institutions with policy making head offices several thousand miles away.

The degree of conflict increases when the global banks, include in their geographical structure small countries commonly referred to as offshore financial centres (OFCs). Such OFCs are numerous throughout the world, and typically very dependent upon a successful financial sector providing a significant economic contribution to the country.

It follows that an incident of money laundering or terrorist financing occurring in an OFC could have a significant negative impact upon the integrity of the financial system of that country.

This paper discusses the impact of such conflicting objectives from the viewpoint of the expectation by regulators to apply robust supervision.

OFFSHORE FINANCIAL CENTRES: THE BACKGROUND

According to the Tax Justice Network[1] between US$21 trillion to US$32 trillion of private wealth is located untaxed or lightly taxed in countries throughout the world. Those countries with light taxes are referred to as OFCs, or more emotively, as tax havens.

There are many good reasons for investors to take advantage of financial services and products in OFCs; avoiding tax by setting up effective tax planning structures and by providing privacy of ownership by the formation of asset holding companies. Such asset holding companies reduce the risk of litigation resulting in asset forfeiture, and calm the fear of kidnapping and ransom requests faced by residents of, for example, Central and South American countries.

Privacy is, however, synonymous with secrecy. It is the aspect of secrecy that has attracted the most attention in recent years when the larger countries such as the United Kingdom and the United States have expressed concern over the alleged significant levels of lost tax revenues through tax evasion. The ease by which the placement of assets and income in offshore shell or anonymous companies, structured with an opaqueness of ownership, is blamed as the cause.

Bodies such as Transparency International[2] and the previously mentioned Tax Justice Network have become vociferous in their campaign against corruption, citing the misuse of anonymous or shell companies as the vehicle to hide assets, acquired not only by tax evasion and the proceeds of drug sales, but other crimes, such as human trafficking and smuggling.

THE REGULATORY FRAMEWORK

The anti-money laundering and combating of terrorist financing regulatory framework is based upon the recommendations[3] issued by the Financial Action Task Force (FATF).

FATF was established by the G-7 Summit held in Paris in 1989. Recognising the threat posed to the banking system and to financial institutions, the G-7 heads of state or government and president of the European Commission convened the Task Force from the G-7 member states, the European Commission and eight other countries.[4]

The FATF and the nine FATF styled bodies now embrace 192 countries throughout the world.

Revised recommendations[5] were issued in 2012 and provide the baseline for the

legislation set in each country. Each country is expected to tailor implementation to its own specific environment and money laundering and terrorist financing threats.

The requirement to reach FATF standards has gained increasing momentum for all member countries. The FATF and its FATF-style regional bodies (FSRB) undertake peer reviews of co-members, which broadcasts publicly that their AML/CFT regimes are either deficient or up to standard. FATF members are encouraged to look upon those countries that fail to move steadily towards full compliance with caution; the rationale for caution being the heightened propensity of a deficient country to enable the movement of illicit funds. Such movement of illicit funds into OFCs can, when discovered, damage significantly the reputation of that OFC, and to a lesser extent the reputation of their peers.

Regulators of the OFCs are coming under increasing pressure through their governments and their peer countries to meet the FATF standards. It follows therefore that the regulator, through its supervisory and regulatory regime, must drive effective implementation of the FATF recommendations.

CONFLICTING VIEWS ON RISK

The impact of money laundering and terrorist financing risks occurring in an OFC is loss of confidence leading to reluctance by genuine investors to use the jurisdiction as a country to invest. The impact on the small country can be significant and significantly damaging to the local economy.

Both the regulator and the financial institutions play a key role in the protection of the integrity of the financial system in the country. Beyond this key role there comes the conflict of objectives between the needs of the financial institution to operate cost efficiently, against the regulator tasked with holding financial institutions to the highest standards. Benchmarking countries globally and in particular against their peer group of OFCs is paramount to attracting legitimate investors.

Both regulators and financial institutions will apply a risk-based approach to compliance objectives due to constraints of financial and human resources, and the resultant need to apply focus to areas of critical risk impact. Nevertheless, the temptation of the financial institutions to play down the levels of risk to justify dilution of risk management processes is very likely.

The challenge to regulators is managing the conflict of objectives, with financial institutions being less concerned over the reputation globally of the country and having greater concern over the effective management of costs.

FINANCIAL INSTITUTIONS: THE RESPONSE TO COST CHALLENGES

As the offshore market has grown, financial institutions face cost pressures arising from both the need to provide technologically progressive products and delivery channels as well as the increasing cost of compliance as a result of growing regulatory scrutiny. In the PwC *2016 Global Economic Crime Survey*,[6] reference is made to the study by WealthInsight[7] in which it is stated that 'Global spending on AML compliance is set to grow to more than $8 billion in 2017.'[8] The PwC survey goes onto say 'But many balk at increasing compliance spend — notwithstanding the cost of enforcement actions and large scale penalties resulting from compliance failures."[9]

In response to the demands to reduce costs, outlets of financial institutions in the OFC have become predominantly sales focused with operations and compliance departments centralised, most likely in a different country.

Because of factors of size of activity in an OFC, relative to group corporate activity, it

can be easily argued that the likelihood of an ML/TF event occurring would be considered in the lower ranges. The impact by way of reputational damage or financial loss can also be assessed as low for similar reasons.

By virtue of lower risk rating, contraction of resources allocated to ML/TF risk mitigation as well as oversight by the various risk management disciplines has occurred. The low risk rating would support the decision that a high level of monitoring would not be cost effective in areas where impact and likelihood of a risk event occurring is low.

TRANSACTION MONITORING: AN EXAMPLE

In the context of financial institutions, the *raison d'être* for the FATF recommendations and the subsequent legislation, is the identification of unusual or 'red flag' customer-related financial activity. After further analysis, such unusual activity may lead to disclosures to law enforcement[10] to investigate further. It follows that the effective monitoring of customer transactions is a key component of the fight against organised crime and the financing of terrorism — 'Follow the Money.'

In this example of transaction monitoring we shall focus on the receipt of incoming international payments using wire transfers, by a global bank with operations in an OFC. Historically, in such an environment each branch processed incoming wire transfers from receipt of details from the relevant correspondent bank. The branch with in-house controls examined the transaction in real time as a point of entry control. Transactions were further examined manually the following day after posting to customer accounts. In both cases the control objectives were to identify unusual activity that deviates from norms relative to that customer or customer type. After investigation, the unusual activity may be deemed suspicious and disclosed to law enforcement.

The strength of the point of entry control was the opportunity to prevent illicit transactions entering the system. For many years the branch based operations served the business well with the in-house branch officers effectively placed to have sufficient knowledge of their customers to determine if activity was suspicious. In turn, branch-based management was able to perform oversight controls.

Centralisation has created a different dynamic. Payment information from the correspondent banks has been diverted to a centralised processing centre serving multiple countries. With a focus on speed of delivery and good customer service, the processing centre will have the mandate of straight through processing. Customer accounts will be credited at the time of entry, with limited manual intervention.

Focus on screening takes on a following day control, by way of automated rules-based interrogation of the transactional database. Rule breaches flagged as alerts are investigated remotely from the account holding branch, and more importantly, remotely from those members of staff with the greatest knowledge of their customers and hence able to relate the transaction to expected and reasonable activity of that customer.

From a customer service, operational efficiency and cost point of view, the financial institution has achieved a good result. Not so the regulator who can be concerned over potential dilution of control effectiveness, with heavy reliance upon the automated transaction monitoring system.

The regulator has every right to be concerned. The concern driven firstly by the changed positioning of the controls to a centralised environment and secondly by the effectiveness of the automated transaction monitoring system. Concern is further

increased by the practical difficulty experienced by the regulator gaining a level of satisfactory assurance of strong control.

Typically, automated transaction monitoring systems generate a high number of false positives which have to be investigated and screened leaving transactions requiring deeper analysis and referral to the account holding branch. The operational risk failure to process alerts in a timely manner is exacerbated by virtue of the volumes involved. The buildup of unexamined alerts was a situation that attracted criticism from the US Senate Permanent Subcommittee on Investigations in their 2012 report on HSBC, when it was cited that a backlog of over 17,000 un-reviewed alerts existed.[11] HSBC was notably fined in 2012 a record US$1.9 billion by US regulatory authorities for poor transaction monitoring activity as well as other AML compliance violations.

The movement of the first line of defence to the centralised unit places emphasis on oversight and how it was to be applied. Adding further to the centralisation model, many financial institutions implement a centralised compliance unit, which as the second line of defence, has the responsibility to assess the effectiveness of the transaction monitoring system including the end-to-end process of the transaction monitoring department. Scope of the compliance department must not only assess the effectiveness of the decision making around the alerts, but also the pace of review and how management ensure that all alerts are cleared daily and no backlog exists.

Internal audit as the third line of defence is typically expected to provide the board, or audit committee of the board, with assurance on the effectiveness of the compliance function.

As a consequence of the cost challenges faced by the financial institution, both internal audit and the compliance department must operate efficiently through a risk-based approach. Based upon their risk assessments, internal audit and compliance determine the frequency and intensity of their assurance work within the constraints of cost and time.

A key driver to the risk assessment is the impact experienced by the financial institution should a risk event occur. From the viewpoint of the centralised units, the risk event considered most concerning should it occur is money laundering through large operational units with high volumes and high value transactions. Conversely, the impact of a money laundering event in a small OFC is unlikely to be assessed as high on the scale of impact.

The consequence of the viewpoints of impact is that the effectiveness of the controls to manage the ML/TF risk pertaining to the small OFC is likely to attract only a limited level of scrutiny by the financial institution. Such a situation is a clear example of the conflict between the financial institution and the regulator in meeting their respective objectives.

Turning more specifically to the effectiveness of the automated transaction monitoring system, the global consulting UK consulting firm Protiviti[12] adds further gravitas to the concern of the regulator.

In the November 2013 report by Protiviti, 'Views on AML transaction monitoring systems,'[13] the global consulting firm highlighted key institutional challenges that come with the deployment of the transaction monitoring system (TMS). The report refers to the challenges faced by financial institutions to acquire and implement an automated transaction monitoring system.

The Protiviti paper cites wide ranging critical challenges including the following.[14]

On selecting an AML transaction monitoring system:

- 'Management often has unreasonable expectations about how a vendor's TM system can improve the institution's TM programme.'[15]

On enhancing AML transaction monitoring scenarios by leveraging customer segmentation:

- 'Lack of accurate KYC data inhibits leveraging KYC information such as customers' occupation, demographics, expected level of transaction activity, etc. When these attributes are not readily available, segmenting customers into meaningful buckets that group together customers with similar traits becomes challenging, if not impossible.'[16]

In addition, the PWC Global Economic Crime Survey 2016[17] mentioned earlier in this paper has stated that:

- 'More than 25% of financial services firms have not conducted AML/CFT risk assessments across their global footprint'.[18]
- 'Only 50% of money laundering or terrorist financing incidents were detected by system alerts'.[19]

The conclusion to be drawn is that AML compliance continues to be a significant challenge to financial institutions and to the regulators. Furthermore, the implementation of an automated transaction monitoring system does not provide, with ease, the panacea to the challenges of AML compliance.

THE CHALLENGE FACING THE REGULATOR

The views of the level of inherent risk, and the resultant frequency and intensity of the assurance work by the compliance and internal audit departments of the financial institution work applied to any one jurisdiction, may not match the expectations of the regulator. The local regulator has a clear responsibility to protect the financial stability and reputation of the country.

In discharging its mandate to protect the reputation of the country from abuse by money laundering and terrorist financing, the regulator will be looking for a commensurate level of supervision and compliance by the financial institution. The dilution of the control environment described in the example is the risk response by a financial institution looking to achieve cost effective compliance in a country that may not figure high in their volume of market representation.

In seeking assurance of the effectiveness of the AML regime of a financial institution, the regulator is obliged to recognise:

- The front line staff will be in the best position to understand the rationale and typical financial activity of their customers; however, this position is weakened by the inevitable focus on sales. AML/CFT training is often considered as secondary to sales training.
- Approaches for business which are aborted, possibly for early red flags such as reluctance to provide due diligence information or negative news from open sources, are only seen by the front line staff. Particularly in an offshore environment, aborted approaches are a rich source of suspicious activity as criminals look for the 'weakest link' to enter the financial system.
- The examiner must assess the process of setting and managing the rules of the transaction monitoring system and consider, most importantly, their relevance to the local environment. The importance of relevant local rules attracted criticism by the US Senate Permanent Subcommittee on Investigations in their 2012 report on HSBC.[20]
- The examiner will wish to assess the quality of the controls to ensure complete and accurate transfer of transactions into the interrogation software.
- The examiner requires assurance on the competency of the manual process of

identifying suspicious activity which will include determination and treatment of false positives.
- The local money laundering reporting officer (or Bank Secrecy Act[21] (BSA) officer) is charged with the unfettered responsibility to report suspicious activity. The examiner must establish how, in a remote centralised environment, this is achieved and in turn supervised.
- Typically, the regulator would rely upon internal compliance and internal audit reviews to inform their examination. Internal audit and compliance determine their review timetable on the perception of risk and the regulator may be unable to force the frequency and scoping of such reviews.

CONCLUSION

The end-to-end process commencing with incoming wire transfer payment information from the correspondent bank, through the centralised units to suspicious activity reporting must be in the regulator's scope when assessing effective compliance, by the financial institution, with both legislation and best practices. The local regulator's mandate to protect the country remains constant.

The one changing factor is that the financial institution itself is driven by competing priorities of achieving cost efficiencies and the need for regulatory compliance.

The pursuit of cost efficiencies has resulted in organisational structures that weaken the value, to the offshore regulator, of both compliance and internal audit.

The cause is predicated upon the conflicting viewpoints of money laundering and terrorist financing risk, more simply referred to as 'risk impact is in the eye of the beholder'. It is clear from the regulatory and policy maker view that risk has to be assessed to a level of detail that drives effective oversight by the head office. The converse being that the head office of the financial institution has a view of risk in the smaller branches and subsidiaries as of lesser impact to the group as a whole, and hence there is less appetite to invest in the oversight and compliance regimes.

The reality is that there is evidence, referred to in this paper, that there is the distinct possibility that unidentified ML/TF risk lies within outlying subsidiaries and branches.

The compliance issues faced by HSBC are symptomatic of a deficient head office and foreign subsidiary/affiliate relationship. The report[22] by the Permanent Subcommittee on Investigations of the United States Senate cites weak AML/CFT controls throughout the group, particularly the affiliates HSBC Bank USA NA and HSBC Mexico.

More generally, the concern faced by the regulator of the OFC is very real but difficult to manage. The relative scale and difficulty of the small country regulator wishing to challenge and influence large global financial institutions is clear to see. The difficulty in this challenge is exacerbated by the geographical remoteness and limited budgets of the regulator to visit and undertake on-site assessments of centralised units.

SOLUTIONS

The diversity of interpretation of risk is an issue driven by cost. Any solution must involve a meeting of the minds by the respective stakeholders. Increased consultation must commence and must bring to the table:

- A meaningful examination and challenge of risk from the viewpoint of all stakeholders. To achieve this, not only should the risk assessment be considered, but the underlying assumptions and source data challenged from every viewpoint.
  - Are risk drivers and actual experiences sufficiently wide ranging?

  - What is history of actual money laundering leading to prosecution?
  - What are the experiences by the supervisory, internal audit and compliance stakeholders in relation to compliance standards?
- What is the experience of the country being used as a conduit for money laundering or terrorist financing even though predicate crimes are not prevalent in the country?
- As described in the FATF guidance 'Risk based approach for the banking sector',[23] would risk assessments performed on specific products or lines of business, delivery channels, customer categories and operational processes, enable head office to selectively target compliance work on higher risk areas thereby controlling cost but continuing to maintain focus?
- Cooperation between regulators should be utilised. Do the home and host regulators have similar or differing views on the risk of centralisation within their own spheres of responsibility? Every effort must be made to resolve differences in risk assessments to equal satisfaction.
- The potential impact of a more aggressive stance by the local regulator in assessing the approach to oversight by head office must be considered. The impact from increased supervisory work may of course be an increase in licensing fees for the banking sector.

In summary, working towards solutions will require concessions on both sides in the context of maintaining the overarching common objective of compliance with local legislation.

Author's note

The views expressed in this paper are the personal views of the writer. The content of the paper does not contain any endorsement or implied accuracy by the writer's employer.

References

(1) Tax Justice Network (2015) 'The offshore game', 14th April, available at: http://www.taxjustice.net/topics/inequality-democracy/inequality-tax-havens/ (accessed 28th April, 2017).

(2) Transparency International, available at: https://www.transparency.org/. One global movement sharing one vision: a world in which government, business, civil society and the daily lives of people are free of corruption (accessed 28th April, 2017).

(3) FAFT (2012) 'Recommendation 20, Reporting of suspicious transactions; FATF 2012 recommendations', available at: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html (accessed 28th April, 2017).

(4) FATF, 'History of the FATF', available at: http://www.fatf-gafi.org/about/historyofthefatf/ (accessed 28th April, 2017).

(5) FAFT, ref. 3 above.

(6) PwC, 'Global economic crime survey 2016', available at: https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html (accessed 28th April, 2017).

(7) See: http://www.wealthinsight.com/About/ (accessed 28th April, 2017).

(8) PwC, ref. 6 above.

(9) *Ibid*.

(10) FAFT, ref. 3 above.

(11) US Senate Committee on Homeland Security and Governmental Affairs (2012) 'US vulnerabilities to money laundering, drugs, and terrorist financing: HSBC case history', Permanent Subcommittee on Investigations United States Senate, 17th July, p. 31, available at: https://www.hsgac.senate.gov/subcommittees/investigations/reports?c=112 (accessed 28th April, 2017).

(12) See: https://www.protiviti.com/US-en/about-us

(13) Protiviti, 'Views on AML transaction monitoring systems', available at: https://www.protiviti.com/US-en/insights/wp-views-aml-transaction-monitoring-systems (accessed 28th April, 2017).

(14) *Ibid*.

(15) *Ibid*., p. 1.

(16) *Ibid*., p. 8.

(17) PwC, ref. 6 above.

(18) *Ibid*., p. 3.

(19) *Ibid*., p. 42.

(20) US Senate Committee on Homeland Security and Governmental Affairs (2012) 'US vulnerabilities to money laundering, drugs, and terrorist financing: HSBC case history', Permanent Subcommittee on Investigations United States Senate, 17th July, p. 55, available at: https://www.hsgac.senate.gov/subcommittees/investigations/reports?c=112 (accessed 28th April, 2017).

(21) Further clarification on the Bank Secrecy Act can be found at https://www.fincen.gov/resources/statutes-regulations/fincens-mandate-congress (accessed 28th April, 2017).

(22) US Senate Committee on Homeland Security and Governmental Affairs (2012) 'US vulnerabilities to money laundering, drugs, and terrorist financing: HSBC case history', Permanent Subcommittee on Investigations United States Senate, 17th July, available at: https://www.hsgac.senate.gov/subcommittees/investigations/reports?c=112 (accessed 28th April, 2017).
(23) FATF (2014) 'Risk-based approach guidance for the banking sector', available at: http://www.fatf-gafi.org/topics/fatfrecommendations/documents/risk-based-approach-banking-sector.html (accessed 28th April, 2017).