The Continuing Fallout From the 1MDB Case: Implications for Singapore and Hong Kong

As investigations into the 1Malaysia Development Berhad (1MDB) corruption scandal continue to spread across the globe, the United States Department of Justice (DoJ) has said that at least US$3.5 billion has apparently been stolen from the fund, which is a Malaysian state investment vehicle set up to promote economic development.¹ Between 2009 and 2015, monies were alleged to have been laundered from the fund through a complex web of opaque transactions and fraudulent shell companies located in tax havens such as the Seychelles and British Virgin Islands, and through reputable international financial institutions across the world, situated in financial centres such as Singapore, Switzerland, Luxembourg, the United Arab Emirates and the United States.

This paper explores the ongoing fallout from this event; pinpointing areas of greater scrutiny from regulators, as well as offering some advice on what actions financial institutions can take to enhance their internal anti-money laundering (AML) controls.

Regulatory Inspection and Oversight

The 1MDB case has had broad implications, not only for Malaysia, but also for other jurisdictions. Singapore in particular was caught in the fallout as investigations by the Monetary Authority of Singapore (MAS) revealed 1MDB-related funds flowed through multiple financial institutions in the city state, made possible through lapses and weaknesses in the firms’ anti-money laundering controls and processes. These breaches were so serious at one Singapore licensed bank, BSI Bank Limited Singapore, that in May 2016 the MAS withdrew its license as a merchant bank.² Further, on October 11, 2016, the MAS ordered another Swiss bank, Falcon Private Bank, to close over alleged serious anti-money laundering failings and improper conduct by senior managers relating to the 1MDB case. Falcon was also fined S$4.3 million (U.S.$3.1 million).³ At the same time, the MAS fined UBS and DBS Bank a combined total of S$2.3 million (U.S.$1.7 million) for allegedly breaching AML requirements and control lapses. These are among the highest fines the MAS has levied for AML violations.

In the introduction to the regulator’s 2015 annual report publication, highlighting the unavoidable activities of money laundering and terrorist financing, MAS managing director, Ravi Menon, described illicit financing risks as “part of the karma of an international financial centre.” He added that while regulatory scrutiny will increase, specifically for Singapore, no regulatory change is expected following the 1MDB fallout since regulations are “already very strict and on par with global standards”, in light of enhancements undertaken for FATF purposes as seen in the 2015 MAS 626 publication and subsequent guidance notes.

Menon remarked further that it is: “Neither realistic nor desirable to expect the MAS to police every single transaction or activity” in the financial markets. Rather, the regulator places the responsibility to instill high standards of risk management controls and proper conduct with each financial institution, predominantly with senior management. The MAS further does not intend to force the development of compliance culture through enforcement action only, reminding firms that it grants banking licenses with the “underlying intention that financial institutions will operate within the regulatory framework, and a culture of compliance should develop organically within an organisation, to become living and breathing through a desire to do the right thing.”

While the regulator does not intend to make any specific regulatory changes following the recent fallout from the 1MDB case, the MAS has taken clear steps to increase its anti-money laundering (AML) and counter terrorist financing (CFT) expertise. On August 1, 2016, the MAS formed a dedicated enforcement department to combat money laundering and strengthen enforcement, with the intention of enabling regulator to take a more targeted approach to AML/CFT by consolidating supervisory resources. By sending specialist teams on-site for focused inspections, the MAS will begin to conduct more intrusive inspections of financial institutions. Equally, within the region, the Hong Kong Monetary Authority (HKMA) is currently hiring to grow its AML investigation and enforcement teams.

Finally, the sophistication of the inspection teams should not be underestimated. Regulatory officers coming on-site for inspections will understand the business, know how the regulations should be applied in practice, and ask the right questions.

**Regulatory Focus Areas**

There has been a significant increase in regulatory focus on AML issues in both Singapore and Hong Kong:

1. **Enforcement Actions**

According to the 2015/2016 MAS annual report, there has been a six-fold increase in inspections of AML/CFT processes at financial institutions; increasing from 108 inspections between 2010 and 2013, to 608 inspections between 2013 and 2016. This growing rate of supervisory inspections is not something that financial institutions should view lightly. Prior to the BSI case, enforcement action was undertaken in a less public manner in Singapore. Financial institutions were not “named and shamed” through public censures or fines. It is understood that limitations were imposed instead until remediation was performed and independently verified as satisfactory. This approach allowed financial institutions to raise their compliance standards with regulator support. However, the enforcement action taken by the MAS in May 2016 against BSI was a game changer for the regulator. BSI had committed repeated violations, and the MAS’ “cannot and will not be tolerated” approach was a significant development in enforcement action.

---


Going forward, as mentioned in the MAS' latest annual report, the regulator will:

- Focus on the implementation of AML/CFT compliance by financial institutions
- Enhance AML/CFT supervision. The MAS has already stepped up inspections and noted that financial institutions are devoting more resources to AML
- “Name and shame” financial institutions that persistently or egregiously breach AML regulations
- Use monitoring tools and data analytics to enhance market surveillance, to help identify potential misconduct, manipulative trading behaviour or to detect patterns across suspicious money laundering transactions, as well as to investigate specific offences. For example, the MAS is exploring the use of machine-learning algorithms to identify manipulative trading behaviour in the capital markets or to detect patterns across suspicious transactions that could indicate money-laundering activity.
- Work closer with the industry, increasing engagements to share perspectives on emerging risks and typologies, as well as best practices on how to mitigate them
- Foster greater cooperation with regulators of other financial markets

By comparison in Hong Kong in 2015, the HKMA announced its first ever public disciplinary action under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO) against a large foreign bank. This incident was highlighted by the HKMA as “a case of internal control failures relating to AML/CFT systems.” On the back of these internal control failings, the bank’s Hong Kong branch was issued a formal reprimand, fined HK$7.5 million (U.S.$1.0 million) and required to submit a report on the sufficiency and effectiveness of its remedial plan to address the contraventions of the AMLO.

The HKMA has used this example “to send a clear message to the industry that all authorised institutions should have effective AML/CFT systems and controls in place to, among other things, detect and report suspicious transactions based on their knowledge of their customers”, adding that “the HKMA will take appropriate enforcement action to deter any lapses in this regard,” Meena Datwani, the Director-General (Enforcement) of the HKMA, said at the time. The HKMA has announced that there are several ongoing AML investigations with other financial institutions.

2. Compliance Culture, Values and Ethics

Many of the financial institutions caught up in the 1MDB investigation were widely considered to have strong ethical and compliance cultures with the necessary processes, experienced staff, and controls in place. In certain recent cases investigated by the MAS and HKMA, the compliance teams were recognised by the regulators as having asked the right questions concerning suspicious transactions but not receiving satisfactory answers.

Nonetheless, any failure to mitigate risks or identity weak controls is taken seriously by all regulators, regardless of organisational size or structure. The fact that the right questions were asked may be a mitigating factor, but the lack of satisfactory responses that resulted in systematic and “substantial breaches” shows a deficiency in the compliance culture.

Compliance frameworks need to be constantly evolving to be effective at all levels of an organisation, with support and endorsement from senior management. A noncompliant culture within management, or indeed messages that contradict the compliance culture, will undermine the effectiveness of these controls. The enforcement action that has been taken against BSI supports this message. Management needs to increase scrutiny of their financial institution's risk management processes and internal controls, including understanding and owning the risks, through ongoing reviews and monitoring. It cannot be left solely to the internal audit function or other lines of defence.
Further, while a compliance culture should be driven by senior management, all employees have an individual responsibility to ensure compliance. This point in particular was addressed in the revised MAS 626 AML Notice and Guidelines issued in 2015, which explicitly state that while management must provide the tools to create a compliance culture, the ownership for AML rests with the first line of defence.\(^8\)

It remains to be seen how financial firms can and will align first-line incentive programs to promote a culture of compliance. Not enough has been done to tackle this so-called “schizophrenia of compliance.” Employees are required to take risk to generate profit, and people in the first line still struggle with the conflict and pressure to achieve; sometimes regardless of the consequence of breaching policy and procedure. Although many lessons have been learned about the dangers of P&L driving culture within the organisation, specifically following the collapse of Barings Bank caused by rogue trader Nick Leeson in 1995, rogue traders continue to exist – Yasuo Hamanaka at Sumitomo in 1996, Jerome Kerviel at Société Générale in 2008, and as recently as 2011, Kweku Adoboli at UBS. The bottom line still drives the personal objectives of some rogue employees, and how that profit is reached is secondary to the organisation’s compliance culture.

The MAS stressed in its 2015/2016 Annual Report that “boards and senior management in particular must send a clear signal that profits do not come before values and ethics. There can be no room for flexibility in ethical standards.”\(^9\)

The importance of global oversight of foreign branches should also be stressed. Governance and compliance culture must be appropriately implemented and translated throughout the organisation. Too many times, foreign branches have become secondary to the issues impacting the head office and, to an extent, foreign branches have been left to their own devices to implement an appropriate governance, risk and compliance framework. This has become a big focus area in enforcement actions. Global management teams of financial institutions need to be aware that any failings in overseas branches will have a direct impact on their reputation with their home regulator.

3. AML Controls Including Monitoring

The key areas addressed on the AML issues are not dissimilar to those we have seen in other regions within comparable regulated markets, which are (but not limited to) failures in the following areas:

1. Client on-boarding and Know Your Customer (KYC)
   - Ultimate beneficial owner (UBO) identification
   - Complex ownership structures
   - Purpose of account
   - Source of wealth
   - Source of funds

2. Transaction monitoring
   - Purpose of payments
   - Relationships of third parties
   - Private banking accounts with high volume transactions
   - Analysis and timely closure of alerts (including escalation)
   - Suspicious Transaction Reporting (STR) procedures and record keeping
   - Reassessment of client AML risk and continuation of relationship based on transaction monitoring alerts
   - Continuous improvement based on regular risk assessment

To assess their risk mitigation controls, firms should take steps to review their AML enterprise risk assessments in fine detail to ensure that their entire AML framework is sufficient. Importantly, firms should ensure that the assessments are re-evaluated should there be any changes in areas such as the business model, client base, product and services or delivery channels.

---

There must be active ongoing monitoring of customer relationships and use of the information received to realign client risk ratings. In this regard, the effectiveness of transaction monitoring screening scenarios and thresholds will likely become a key focus area of review by regulators in the next 12 months, along with the testing of sanction screening systems. In particular, many financial institutions have bought off-the-shelf systems for these purposes, but these systems may not have been tested for operational effectiveness or applicability to the business model, or appropriately reviewed on a periodic basis to assess the performance of the scenario. Importantly, in the case of the BSI enforcement action, it clearly showed that monitoring the firm's controls lapses must not be left to the regulator to identify.

Firms will also now be assessed on how they respond to findings from active monitoring. Merely filing a Suspicious Transaction Report (STR) is not where the duty of the financial institution begins and ends. Filing STRs for defensive purposes is not the answer either. In the 2013 Singapore client tax risk reviews, some 49.4% of STRs were filed for defensive purposes, including purpose of account unknown, unknown source of wealth and incomplete tax reviews. This shows that incomplete risk assessments were performed and that there is a lack of real client understanding and underlying KYC requirements. Firms need to assess, within a controlled framework, the reasons for filing an STR, and maintain a complete record of their decisions where not to file a report.

Strengthening AML controls may be a significant investment, but financial institutions need to reinforce management commitment and set aside sufficient budget to address these matters, while also balancing costs and returns over the longer term.

4. Remediation
Finally and importantly, firms need to ensure they undertake adequate remediation work where lapses in controls are found. There can be no quick fixes to remediating audit and regulatory findings. Remediation must be done with precision, targeting the root cause, and enhancing the controls across the entire end-to-end process/control framework, while also testing for operational effectiveness. Many firms are introducing compliance quality assurance teams within their compliance frameworks, the third line of defence can also play a key role here. Firms can enhance their risk management but implementing an audit program that focuses on testing all AML controls, especially those that have been identified by regulators as being issues, as well as modifying the program to account for newly-identified risks, regulatory issues in the press, and thematic issues.

5. Key Takeaways
Financial regulators around the world are stepping up monitoring activities and taking tougher action when firms breach AML rules. Financial institutions can adapt to meet more stringent regulatory expectations in the following areas:

1. Foreign branch governance frameworks should be reviewed, and management information system (MIS) reporting enhanced to support this
2. Greater ownership at board and senior management levels of key risks, clear documentation of escalation procedures, and key performance indicators on AML imposed on all employees
3. Enhance performance of detailed AML enterprise risk assessments and regulatory gap analysis, including development of risk assessment matrices for client, geographic, product and delivery channel risk, with ongoing evaluation of risks should changes occur such as to the business activities or client scope
4. Establish operationally effective compliance procedures, including the AML 101 of ensuring, to the level required by regulation, that customer due diligence requirements are completed prior to establishing business relationships
5. Establish and maintain effective procedures for identifying whether customers or their beneficial owners are politically exposed persons (PEPs)
6. Continuously monitor business relationships with customers, including the development of transaction monitoring frameworks with scenarios tested for operational effectiveness and applicability to business activities
7. Design quality assurance testing programmes
8. Conduct AML and CFT training on an ongoing basis, which is targeted and tailored to the specific risks that exist in each business line and custom-made for first, second and third line, respectively. This training should not be a one-off annual exercise.

How Protiviti Can Help

Protiviti has a dedicated Anti-Money Laundering (AML) team within its Regulatory Risk Consulting practice. The core members of our AML practice are former financial institution regulators, financial institution compliance officers, fraud and forensic specialists, technology experts, and individuals with hands-on experience working in financial institutions of all types. Protiviti’s AML team members have considerable experience advising institutions of all types on the design and implementation of their AML/CFT Compliance Programs, conducting independent tests of AML/CFT Compliance Program effectiveness and conducting money laundering investigations.

Contacts

Suneet Gorawara
+852.2238.0486
+852.5630.5080
suneet.gorawara@protiviti.com

Oonagh McKinley-Hutchinson
+852.2238.0424
oonagh.mckinley-hutchinson@protiviti.com

George Brown
+852.6318.2902
+852.2238.0481
george.brown@protiviti.com

Ronita Dutta
+65.6309.5950
ronita.dutta@protiviti.com

For AML/CFT compliance updates and news, please visit www.protiviti.com/AML.

Our team helps companies with the following solutions:

- Design and Implementation of AML/CFT Risk Assessments
- AML Program Development, Implementation and Review
- AML/CFT System Vendor Selection and Utilisation
- Model Assessments and Data Validation for AML/CFT Systems
- OFAC Sanctions Compliance Program Design and Reviews
- Money Laundering Investigations
- Independent Testing of AML Programs (Sanctions, Transactions Monitoring, Validation)
- Regulatory Response Advisory
- Program Remediation
- Focused Training (Design, Development and Delivery)