KPMG

Current issues in Anti-money laundering and Anti-terrorist financing in Bermuda

August 2019

kpmg.bm

Introduction

On March 7, 2019, KPMG hosted a current issues discussion on Anti-Money Laundering (AML)/ Anti-Terrorist Financing (ATF) with guest speakers from the Bermuda Monetary Authority (BMA or the Authority).

This session was organized following the success of the previous Question & Answer Panel Session on AML/ATF in May 2017. The focus of the discussion of the current issues included topical issues relevant to both regulated financial institutions and the broader market,such as:

- Recent legislative changes in relation to AML/ATF;
- The Caribbean Financial Action Task Force (CFATF) 2018 Mutual Evaluation;
- AML/ATF Supervision and Enforcement; and
- Digital Asset Business.

This document has been prepared based on the discussion during the event and has been validated by the BMA. The views represented in this document are those of the BMA and not those of KPMG.

We would be happy to help with any additional questions you may have.

Regards,

Charles Thresh
Managing Director,
Head of Advisory
KPMG in Bermuda

EVENT DETAILS:

Date:
Tuesday, March 7, 2019

Time:
3:00pm – 5:00pm

Location:
Bermuda Underwater Exploration Institute (BUEI)

Panel:
Chris Brown (BMA),
Katie Duguay (BMA),
Moad Fahmi (BMA), and
Melanie Fullerton (BMA)

Facilitated by
Charles Thresh (KPMG)

Guest speaker:
Shauna MacKenzie (BMA)

Key focus areas

There is a heavy agenda on ensuring Bermuda's alignment with International Standards continues. The focus will include:

- AML/ATF - with the CFATF Mutual Evaluation Review
- The insurance framework - the European Insurance and Occupational Pensions Authority (EIOPA) assessment update for Solvency II
- Qualified jurisdiction designation by the National Association of Insurance Commissioners - Upcoming assessment by the US Authorities
- Forum on Harmful Tax Practices work and Economic substance review by Organization for Economic Cooperation and Development (OECD)
- Review of Corporate Service Providers (CSPs) and Trust Service Providers (TSPs) regulatory regime, in line with standards proposed by the Group of International Financial Centre Supervisors (GIFCS)
- Assessment of COMFRAME principles of International Association of Insurance Supervisors(IAIS)
- Legislative amendments to include changes to insurance rules related to Bermuda Capital Solvency Requirement (BSCR), segregated accounts, reform of Investment funds and business regimes
- Strategies to be reviewed are related to outsourcing and banking
- Financial stability focus on banking resolution and Fintech related developments

Contents

05 **Section 1:**
Anti-money laundering and Anti-terrorist financing
CFATF Mutual Evaluation
Supervisory approach
Regulatory requirements and key updates

14 **Section 2:**
Enforcement
Escalation and enforcement process
Regulatory powers

18 **Section 3:**
Digital asset business
Key risks and opportunities
Supervisory approach

SECTION 1

Anti-money laundering and Anti-terrorist financing

As many of us know the Mutual Evaluation Report has been through its first draft review, can the BMA provide an update as to the status of that report?

The Authority remains encouraged, although the process for the finalisation of the report will be a lengthy one. Bermuda received and commented on the first draft of the Mutual Evaluation Report in November/ December 2018. The National Anti-Money Laundering Committee (NAMLC) and the competent authorities are presently working through comments to the second draft, including final key issues which were due to the Assessors on May 3, 2019. The final report will be discussed at the CFATF Plenary in November 2019 and finally at the Financial Action Task Force (FATF) Plenary in 2020.

In conjunction with the CFATF Mutual Evaluation, there have been quite a few legislative updates and changes since our last event in 2017, including extending the scope of the regulatory reach. What are some of the recurring trends across sectors that you are observing when conducting AML onsites where entities are 'non-compliant'?

The majority of legislative changes over the last two years have been made to ensure complete alignment to the FATF Recommendations. The BMA disseminated a separate bulletin summarizing these changes to regulated entities who attended the BMA's sector specific outreach sessions in Q1 2019.

Based on the BMA's observations, here are some key topics that organisations should ensure that they have in hand:

- Appropriate business risk assessments, to ensure AML/ATF compliance programs are aware and focused on the business-specific higher risk items and that this carries through to customer risk assessments.
- AML/ATF and Sanctions Policies & Procedures (P&Ps) that have been reviewed in light of the suite of recent AML/ATF legislative amendments and changes to Bermuda's sanctions regime.
- Ongoing monitoring, with a focus on the identified higher risks according to the risk ratings that have been assigned. This should not be a tick box exercise. AML/ATF regulated financial institutions (RFIs) should be checking that the customer information obtained at onboarding is still valid and the transactions and activity are commensurate with what was expected based on the account profile.
- Clear plans and deadlines to complete any required remediation.
- Training.
- Managing and monitoring AML/ATF compliance.
- Managing outsourced functions.
- Suspicious activity reporting (SARS).

The BMA is also still seeing a need for better management reporting of AML/ATF and compliance issues to the Board

There are a lot of organisations experiencing challenges when determining an appropriate risk-based approach, considering the extent of their operations, size and complexity. One of these challenges arises in relation to the audit requirement per Regulation 17A. Can you clarify or provide guidance as to what the annual audit should consider?

The requirement arising per Regulation 17A for the independent audit itself is not "risk-based" – other than the frequency, where a RFI may determine a particular area may need to be audited on a more frequent basis, nevertheless the independent audit must cover all facets of the AML/ATF program and be conducted at least on an annual basis.

It is acceptable to conduct a series of topic-specific independent audit reviews over the course of the year – provided that in total they cover your entire program–and to then consolidate the outcomes into a single report at the end of the year for the Board's review and action.

The audit is intended to provide an organisation's Board with a document showing "an independent and objective evaluation of the robustness of the AML/ATF framework, and the reliability, integrity and completeness of the design and effectiveness of the AML/ATF risk management function and AML/ATF internal controls framework, and the AML/ATF compliance."

One key requirement is that this is to be an "independent" audit. In practical terms, this means conducted by a person who is independent from the design, implementation and oversight of the AML/ATF program. This could include a quality assurance or testing team, an AML/ATF qualified Non-Executive Director or an individual that is independent of the AML/ATF function. The RFI does not need to have an internal audit department, or outsource this function.

If you outsource this function, you should ensure that independent audit covers the requirements as noted in the Guidance Notes for AML/ATF Regulated Financial Institutions on AML/ATF 2016 (September 2016) (GN) and that the report is of good quality. The scope of the independent AML/ATF audit requirement is covered in the GN 1.75-1.79.

From the BMA's experience, it seems there is a perception that once an organisation has an AML/ATF program in place, customer files are remediated, etc., there is in essence a "steady state", for which "yet another" independent audit will not add a lot of value.Once your client files are remediated, this is not the end of the AML audit requirement.

Based on the BMA's experience in industry, there is rarely a year where nothing changes–your business model, the external regulations, staff turnover are all subject to change. An annual independent audit, properly conducted, will always add value.

Is there any appetite for the BMA to standardize the independent audit review, for example the BMA providing a template which entities have to input certain numbers?

No, the expected scope for audit is clear from the GN 1.75-1.79 and as noted above, it needs to cover the entire AML/ATF program.

Once an enforcement action commences against an entity, particularly one that is in remediation, does ongoing supervision and remediation cease?

Ongoing supervision and remediation activities are seen as separate and distinct functions at the BMA, that run parallel to any Enforcement department activities. A referral to Enforcement does not suspend ongoing supervision and remediation.

Where deadlines are imposed on an RFI by Enforcement and AML/ATF or perhaps the prudential supervisor, each deadline should be met. Where necessary, there will be joint meetings held with the RFI and the Supervision and Enforcement teams.

For the licensee, supervision and remediation activities should run parallel to enforcement actions. The licensee should keep the supervision team abreast of ongoing remediation while enforcement activities are ongoing. If the licensee has an enforcement action commenced, it is very important to continue to meet all supervision and remediation deadlines. Effective remediation by an RFI does not preclude the Authority from taking enforcement action with respect to the original failures.

If you receive a warning notice, it is recommended by the Authority that licensees come and meet with Enforcement to discuss the Warning Notice. Although the Authority will require representations against the Warning Notice to be in writing, the Authority encourages discussions to take place with Enforcement. Such discussions are routine and can assist with clarifying issues before the written representations are submitted.

RFI's are advised that the content of written representations is a vital part of the process and great care should be given to their preparation. More information about this process can be found in the Enforcement Guide on the Authority's website.

Another area where change is expected is in relation to how organisations use technology focused solutions to support their compliance function–in terms of Customer Due Diligence (CDD), given the increased use of electronic databases for verification of identity or address, has the BMA seen an increase in the use of such technologies? Does the use of technology inhibit or increase compliance with the Regulations?

The BMA is not seeing an increase in the use of technology in the specific context of identification and verification. The second part of the question – about whether technology inhibits or enhances compliance – is already catered for in the guidance. GN 4.16 states *"Evidence of identity may be in documentary or electronic form. An appropriate record of the steps taken, and copies or records of the evidence obtained to identify the customer, must be kept as per the recordkeeping portion of this guidance."*

As technology solutions emerge in this space, RFIs should keep this guidance in mind as they embrace and incorporate it. It is up to the RFI to ensure that the sources and systems used are in compliance with the Regulations. Technology is an enabler and a tool, it is important to ensure that RFIs apply the same level of common sense and critical assessment towards information provided electronically by third party suppliers as they would to paper documents.

Given that insurance managers have not always been in the scope of the Regulations, some clarity would be helpful in relation to who is considered the customer for AML/ATF purposes? For example, in Segregated Account Companies (SACs), who is the customer, when each cell has a different owner?

Where an Insurance Manager is running a Segregated Account Company, "the customer" whom the insurance manager is managing is the insurer, presumably utilizing a cell or cells in the SAC for this purpose. If that managed insurer is themselves also subject to AML/ATF regulation (for example, they write long-term direct policies), that managed insurer must also in turn know their clients.

As a result of the National Risk Assessment (NRA), it was determined that there are SAC structures identified as a possible risk. The BMA presented a consultation paper in 2018 and is currently working through that feedback.

Part of the legislative updates that took place over the last two-years included the definition of 'Financial Groups' which requires any company that is part of a financial group to implement group wide policies and procedures against money laundering/terrorist financing (ML/TF) which are applicable and appropriate to all members of the financial group, i.e. CDD, Record Keeping, Wire Transfers, Policies and Procedures for sharing information, etc.

Can you provide an example of when a group of companies may be designated as a financial group?

It is important to note that before entities are subject to Regulation 12A (Financial Groups) they would first have to be designated a "Financial Group" by the Minister of Justice. The intent is to do this where you have a parent in Bermuda with subsidiaries either locally and/or internationally.

The key obligation of financial groups in this context is that group-wide policies and procedures are implemented to combat ML/TF which are applicable and appropriate to all members of the financial group. The policies and procedures should be compliant with the requirements set out in Parts 2-4 of the Proceeds of Crime (AML/ATF) Regulations 2008 and follow all of the regulatory obligations of Regulation 12A including the requirement for group level compliance, audit and AML/ATF functions.

Entities who anticipate being designated as a "financial group" should consider their operations with a view to implementing Regulation 12A, including grouplevel compliance, audit and AML/ATF procedures.

For example

Company A

- Headquartered in Munich.
- A Bermuda subsidiary which in turn owns operations in Cayman.
- Per Regulation 12, the Cayman operation must adhere to Bermuda AML/ATF Regulations but that is the extent of "Bermuda" impact. The BMA will accept that the German authorities are regulating the Company at the Group level in Germany.

Company B

- Designated AML Group Headquarters in Bermuda, with subsidiary operations in Cayman, the Bahamas and South Africa.
- Not only do the Cayman, Bahamas and South African operations need to adhere to, at minimum, Bermuda Regulations under Regulation 12, but also the Bermuda Headquarters must take the Group view of the combined operations to assure itself that the Group is managing its Group level risks appropriately. Ref: Regulation 12A & GN 1.57-1.68.

With regard to a company which is incorporated and licensed in Bermuda, but does not carry out any business in Bermuda, and therefore does not have any customers in Bermuda, to what extent must the company comply with the Regulations?

A company which is licensed and incorporated in Bermuda, but does not carry out any business in Bermuda and has no customers in Bermuda must still follow the AML/ATF Regulations. An example of this might be a Bermudian insurer with a long-term direct business licence and customers with life policies that are based in Hong Kong. Operational activities of a Bermuda RFI are undertaken by employees in other jurisdictions, those employees should be subject to the same AML/ATF policies and procedures applied to Bermuda employees. Ref: GN 1.64.

That insurer must follow the AML/ATF Regulations like every other company that is regulated in Bermuda. As the supervisor, the BMA would still, for example, test customer files by electronic means via a secure portal, to ensure that the proper customer due diligence and AML/ATF controls were in place.

At the prior event in 2017, the BMA outlined the steps which should be taken to obtain adequate evidence of Source of Wealth ("SoW"), in relation to pre-existing customers. This included a) research through public information sources, b) verification from third parties such as the customer's bank or lawyer, and c) a self-declaration of SoW by the customer, with some reasonableness testing.

Has there been any change of the BMA's SoW verification?

There has been no change. The BMA still requires adequate evidence of SoW, in relation to pre-existing customers.

What should be the approach when conducting a risk assessment for a low-risk business and lowrisk customers? Is it acceptable to reach a "low risk" conclusion for your business?

The risk assessment process is a critical step in the implementation of an effective AML/ATF program. It is acceptable to reach a "low risk" conclusion, as long as this is properly justified and documented. The BMA would note that in Bermuda's context they would closely examine a business which assesses itself as "low risk" overall.

Customer Risk Rating: In risk rating customers, the RFI should identify the threats associated with the customer as well as the vulnerabilities associated with the product, service, delivery channel and geographic risks associated with the client. Refer to Chapter 2 of the GN and any relevant Sector Specific Guidance Notes for red flags associated with the sector and what questions to ask when determining the customer risk.

Note: The fact that Bermuda provides services to international, high net worth customers, some of whom are non-face-to-face increases the risk of ML/ TF. RFIs should not, therefore presume that only cashbased business is associated with ML/TF and that all other local business is low risk. Sector-specific risks identified in the NRA should be considered before determining that certain customers are "low risk".

Due to the nature of Bermuda's international business, the complicated products/services and structures used, Bermuda is vulnerable to the layering and integration stages of ML. Many of the sectors in Bermuda's financial services industry have been identified as having a high ML/TF risk including Banking, Securities, Corporate Service Providers and Trust Service Providers.

Before concluding that your customer has a low risk for ML/TF, all four ML/TF risk factors (customer, product/service, delivery channel and geographic risks) should be taken into account.

Business Risk Assessment: When conducting an entity-wide or business risk assessment in keeping with Regulation 16(1)(ea), it is important to identify and assess your business inherent risks as well as consider the inherent ML/TF vulnerability of your sector based on the NRA. Similar to the customer risk rating process, conducting a business risk assessment requires the RFI to consider all ML/TF risk factors and tailor the assessment accordingly.

RFIs should consider all relevant risk factors with regard to its customer, products/services, transactions, delivery channels, third party service providers and geographic connections in order to assign inherent risk ratings.

Factors raising the overall risk of your business may include dealings with international transaction flows, high-risk or high net-worth individuals, politically exposed persons, large dollar volumes, a clientele that is predominantly non-face-to-face and the vulnerability of certain products and services.

The RFI should ensure that the method used for risk rating is not egregiously flawed and is sufficiently robust to withstand scrutiny.

After considering all factors, if the RFI has determined that the overall inherent risk of the business is still "low" risk for ML/TF, the RFI should document this with an explanation for the rationale.

Because ML/TF methods are always evolving, the RFI's business risk assessment should be updated at least annually and sufficiently robust in order to demonstrate that the business acted reasonably.

In summary, a properly conducted risk assessment should help an RFI rank and prioritise its risks, provide a control framework for managing those risks, and ensure that compliance resources are allocated to the risk areas where they are needed the most to prevent and suppress ML/TF.

See Chapter 2 of the GN for further information.

Is there a standardised list for assessing geographic risk in Bermuda?

The BMA does not plan to publish a standardized list for assessing countries with a higher geographic risk for ML/TF or corruption.

The lists which RFIs should, at a minimum, take into account when considering geographic risk include: (i) FATF's semi-annual publication of countries which have strategic AML/ATF deficiencies (ii) CFATF high-risk lists (iii) US Department of Treasury's International Narcotics Control Strategy Report (Vol. II) (iv) Basel's AML Index and (v) Transparency International's Corruption Perceptions Index.

What approach should be taken for AML training for staff at different levels in a business?

AML/ATF training should vary depending on their roles and responsibilities. All employees should have a basic general understanding of AML/ATF regardless of function. Management and staff who directly handle customer transactions or instructions should be trained to be alert to circumstances of customers who present a higher risk of ML/TF. Those employees should be aware of their sector's ML/TF vulnerabilities and be able to identify and report anything that gives grounds for suspicion. New staff, temporary and contract staff carrying out such functions should also receive AML/ATF training.

The Compliance Officer is responsible for oversight of the RFI's AML/ATF compliance, thus the Authority expects that the Compliance Officer and Money Laundering Reporting Officer to have an in-depth knowledge of AML/ATF compliance. The Authority expects the Money Laundering Reporting Officer (MLRO), Compliance Officer and Board members to have an enhanced AML/ATF awareness, thus training specific to those roles is strongly suggested.

What is the scope of the new licence requirements for lending businesses? It is noted that the language used is broad in scope and could potentially incorporate any type of lending – for example, investment funds or non-financial businesses issuing loans.

These amendments were passed with standalone lending and leasing firms in mind. To clarify, there is no intention to expand the scope of the new license requirements to the in-house lending that occurs within some larger institutions, e.g. in the insurance or reinsurance sector.

What should be the approach to SARs in other jurisdictions?

Senior Management should ensure that all suspicious transactions or activities occurring overseas but linked with a Bermuda RFI or Bermuda person are reported to the Money Laundering Reporting Officer in Bermuda.

Within a financial group, where a Bermuda RFI's internal SAR to a non-Bermuda parent or head office results in an external report to a non-Bermuda authority, the Bermuda RFI must also make an external report to Bermuda's Financial Intelligence Agency. (Ref: GN 1.64 and 9.49)

What is the correct approach for former Politically Exposed Persons (PEPs)?

The treatment of PEPs is important.

For reference, in the Authority's mission as Bermuda's "Gatekeeper" the Corporate Authorisations team helps to mitigate the reputational risks to the jurisdiction by ensuring that those wishing to incorporate and/or operate financial institutions in Bermuda are properly vetted, observe high ethical standards and are free from criminal activity. The Corporate Authorisations team as Exchange Controller has responsibilities in relation to vetting and retaining information on beneficial ownership of legal persons including approval of share transfers.

A PEP or former PEP, must be declared on the Authority's Personal Declaration forms for all Directors, Officers and Shareholders. For due diligence purposes, the Authority's Corporate Authorisations team takes the "once a PEP, always a PEP" approach.

From a supervision standpoint, RFIs should apply a risk-based approach in determining whether an individual who has been entrusted with a prominent public function but no longer holds that post should still be handled as a PEP from an enhanced due diligence perspective. So "once a PEP, always a PEP" applies for at least identifying such persons. At a minimum, such an individual must be treated as a PEP for a period of one-year after leaving office.

Possible risk factors for determining whether to apply enhanced due diligence (EDD) to an individual as a PEP for a prolonged period of time include:

- The level of (informal) influence that the individual could still exercise;
- The seniority of the position that the individual held as a PEP; and
- The connection (both formal and informal) between the individual's previous and current positions and functions. (Ref: GN 5.103).

Is total net worth required to be verified for SoW?

While conversations about private wealth and source of funds may be difficult, they are necessary.

For the purposes of establishing the source of wealth of a PEP or other relevant person, the source of wealth means the origin of the person's total assets. The information on the source of wealth should provide an indication of the person's volume of wealth and a general understanding of how the person acquired that wealth. The amount of a customer's wealth is important in that it must seem reasonable in the context of the transactions flowing through the account.

The source of a customer's wealth should be verified in circumstances where the RFI determines that enhanced due diligence should be applied, the customer carries a higher risk rating or in order to obtain an understanding sufficient to onboard and monitor the business relationship.

For the purposes of establishing the source of wealth and source of funds of a PEP or other relevant person, RFIs may rely upon declarations by the person, but must apply risk-sensitive measures to verify this information. In particular, when the financial crime risks are high, where there is significant adverse information or there are doubts as to the veracity of the information provided by the customer or beneficial owner, RFIs should validate this information using independent and reliable sources.

Note: An inability of the RFI to verify the person's declaration of the source of wealth or source of funds should be taken into account when establishing the value of the information provided.

In addition, discrepancies between the person's declaration and information obtained from other sources or refusal of the person to disclose relevant information on the source of wealth or source of funds may be considered red flags. Ref: GN Notes 5.110-5.113 and 7.6.

For CSPs, is there any difference in the inherent risk between Bermuda based clients and those from overseas?

Yes, and it is important to take a risk-based approach as well as consider Bermuda's international context and the inherent vulnerabilities of the CSP sector.

The CSP sector serves as one of the major gateways to Bermuda's international financial services sector and a large percentage of its customers are international. The CSP sector has been assessed in Bermuda's National Risk Assessment as having a high overall threat rating, high inherent vulnerability and high inherent ML risk rating.

The inherent ML/TF risk of overseas clients is higher than that relative to Bermuda-based clients. Geographic, customer, product/service and distribution channel risks should all be considered as relevant ML/TF risk factors.

International clients and/or beneficial owners/controllers may be non-face-to-face and others may be PEPs, high net worth individuals and/or individuals from a higher risk jurisdiction. Taken together, these factors would raise the overall risk of the customer.

Depending on the situation, local Bermuda companies may carry a lower risk for ML/TF than that of international customers and beneficiaries. For example, a non-cash based local business with limited international exposure where the owners/controllers are Bermudians and all business is conducted on a face-to-face basis.

Some exceptions to that rule that would raise the overall ML/TF risk to high might include:

- A local Bermuda company where the ultimate beneficial owner and controller is a former Premier of Bermuda.
- A cash-based local Bermuda retail company with large monthly cash flows and international wires that seem to be inconsistent with the industry norms and cannot readily be explained from a business standpoint.
- A corporate entity where there is unusual complexity in the control or ownership structures and the legal structure has been altered frequently without explanation.
- For example: A corporate entity where there is unusual complexity in the control or ownership structures, the legal structure, directors and/or corporate service providers have been changed frequently without good explanation.
- Thus, a customer's overall risk rating should be based on the sum of the customer, geographic, distribution channel and product/service risk taking into account the inherently "high" ML risk of the CSP sector. (Ref: NRA, p. 66)

Enforcement

As part of the normal supervisory relationship, in many cases, non-compliances are addressed and monitored by the AML/ATF Supervision team, and only referred to the Enforcement Department as a final resort.

However, in some cases, egregious non-compliances (including those detected during an onsite) are escalated to Enforcement immediately.

What is the process of how an enforcement action comes to be?

The BMA will not apply its enforcement powers to address every single non-compliance with a regulatory obligation.

Most issues that arise will be addressed as part of the normal supervisory relationship that exists between the BMA and the RFI. Where a firm or individual has failed to comply with statutory requirement(s), it may be appropriate to respond without the need for formal enforcement action. The proactive supervision and monitoring of RFIs and the open cooperative relationship that exists between the RFI and the BMA typically results in a positive supervisory outcome without the need to invoke formal enforcement powers.

It is important to note that the Supervision team also has statutory powers that they may exercise without the need for a referral to Enforcement, for example, they may add, vary or delete any condition imposed upon the Certificate of Registration of an insurer, without the need for a Warning Notice being prepared.

However, typically Supervision and Enforcement will liaise and work together. Supervision may also impose civil penalties for failure to file statutory statements or returns. This is another matter, which falls within the remit of the supervisory powers and does not require formal enforcement action.

Where remedial action has not been undertaken by an RFI or there are repeated breaches of the same nature, Supervision will then refer the matter to Enforcement for consideration.

A matter will be potentially serious if it creates a risk of harm to customers or to the reputation of the jurisdiction as a well-regulated financial centre. Where a matter is referred, Supervision and Enforcement will work collaboratively and agree upon the most appropriate course of action. Matters which are usually referred to Enforcement include:

- Breach of the minimum criteria;
- Breaches of the minimum solvency requirements;
- Issues which relate to the fitness and propriety of an individual;
- Significant failures in corporate governance that pose a risk to the future of the business or the customers/clients/ policyholders;
- Failure to implement a remediation plan; and
- Conducting unauthorized business.

Enforcement considers the facts and decide whether the matter should be presented before the Enforcement Committee or should be handled within the remit of the supervisory powers. If it is escalated, Enforcement prepares the requisite documentation for the Enforcement Committee to consider. The Enforcement Committee then can ask questions, require further clarification of a point, or request further investigation.

Once the Enforcement Committee is comfortable that they are fully informed on the matter, they either accept or reject the recommended enforcement action. If it is accepted, then a Warning Notice is prepared, which is then sent to the entity.

Once an entity receives a Warning Notice they can make representations to the BMA, which is encouraged. This can be a very useful step in the process and can often assist in narrowing the scope of the enforcement action, as applicable.

The Enforcement Committee is made aware of the representations that have been made, and then decide whether to issue a Decision Notice. Entities may appeal a Decision Notice and this is done through the Ministry of Finance.

A referral to Enforcement does not operate to suspend ongoing supervision and remediation; the two processes run parallel and independently of each other.

Referrals to enforcement can take place in a variety of ways, such as when an entity has failed to complete an AML/ATF remediation. In this case how does the BMA verify that the remediation effort has failed and what powers does the BMA have in relation to this?

Supervision will refer identified regulatory issues to Enforcement. Although the majority of the issues are identified as part of the usual supervisory process, matters can also come to light as a result of a referral from outside of the BMA, such as from other regulators, or from the police.

Once the matter has been reviewed or investigated, if such is required, the BMA will communicate with the RFI to advise them of the referral and the communication with the RFI will persist throughout the length of the enforcement action. If there is a criminal element, then, of course, the matter will be referred to the Bermuda Police Service.

Where a suspected breach is brought to the attention of Enforcement, there are formal powers in the Regulatory Acts, Proceeds of Crime (AML/ATF Supervision and Enforcement) Act 2008 and the BMA Act 1969 for the BMA to require by written notice, such information as may be reasonably required for the performance of its functions, i.e. to produce documents, and for the officers of the RFI to attend before the BMA to answer questions.

The BMA has the formal powers to enter the business premises of institutions for the purposes of inspecting the premises, observing the carrying on of business, inspecting and taking copies of any recorded information and for requiring any person on the premises to provide an explanation of any recorded information. Failure to comply with any of these provisions without reasonable excuse constitutes a criminal offence.

Some of the BMA's power to require information extends beyond the regulated community to non-regulated persons.

The BMA can also make an application to the Magistrates' Court for a warrant to enter premises where documents or information are held, or where it has reasonable grounds for believing that if an RFI was required to provide information to produce documents, that it would fail to comply with such a request, or where it believes that if such a request was made that information or documentation would be destroyed.

This represents extreme circumstances and the use of these powers is infrequent, as the BMA are generally able to rely upon the willingness of RFIs to provide information voluntarily.

The BMA also has the power to defer enforcement actions, where representations made by an RFI in response to a Warning Notice have been made which challenge the factual accuracy. The BMA will use the information derived from such an investigation in reaching a decision on whether to proceed further with enforcement proceedings.

Additionally, the BMA may conduct a formal investigation by appointing one or more competent persons to investigate on its behalf and report back on the nature, conduct or status of an RFI's business or any aspect of it, or on the ownership or control structure of the RFI. If an investigator is appointed, written notice of such appointment is provided to the RFI and unless otherwise directed by the BMA, the RFI will pay the costs of the investigation and any expenses incidental to it.

In relation to the wave of legislative amendments that have come into effect between 2016 and 2018, what does this mean for RFIs from an enforcement perspective - what are the key elements that RFIs should be aware of?

- As of September 2018, a new Statement of Principles & Guidance on the Exercise of Enforcement Powers was issued. This replaces the 2010 Statement of Principles in relation to AML/ATF and the 2012 Statement of Principles on the Use of Enforcement Powers;
- The penalties for a breach of AML/ATF regulations has increased from $500,000 to $10 million per breach;
- Enforcement powers are now embedded in the Regulatory Acts and in the Supervision and Enforcement Act;
- Publicity – this is now also embedded in the Regulatory Acts and the Supervision and Enforcement Act, and has been previously, but this has been emphasized since 2016 when the BMA released a statement changing their policy on the publication of enforcement actions. The BMA will now publish, unless exceptional circumstances exist, the name of the entity, the enforcement action taken and the breaches, which triggered the enforcement action.

Does the BMA have any enforcement powers against individuals? What criteria are they assessed against?

Yes, the BMA has the power to take action against individuals. A Prohibition Order will ban an individual from roles in relation to licensees in a specific regulatory sector. The standard of conduct expected of individuals who are directors or individuals who perform functions relating to regulated activity is set out in the Minimum Criteria of the Regulatory Acts and may be supported by Guidance Notes, Statements of Principle and Codes of Conduct.

The BMA has the power to vary the scope of prohibition orders depending on the circumstances of each case. For example, the BMA may seek to prohibit individuals from performing any class of function in relation to the regulated activity in any RFI in the specified financial sector, or it may limit the prohibition functions in relation to that sector.

The scope of the Prohibition Order will depend on the range of functions which the individual concerned performs in relation to regulated activities, the reason why they are not fit and proper, and the severity of the risk which they pose to the compliance level of RFIs and the reputation of Bermuda as a financial centre.

The BMA will take into account some or all of the following matters when considering whether to make a Prohibition Order:

1. The conduct as compared to the standards in the minimum criteria;
2. Whether the conduct was deliberate, reckless, intentional, or inadvertent;
3. The impact of the conduct, including the risks of the entity, customers and stakeholders;
4. The length of time since the conduct occurred;
5. The position and role of the individual;
6. The nature and activities of the RFI concerned; and
7. Was the conduct dishonest, fraudulent or criminal etc.

The BMA can also object to controllers of a licensed entity. The BMA can object to officers and directors at the time of appointment, or at the acquisition of a significant shareholding in an RFI giving rise to "control". The BMA will serve a Preliminary Notice and in the absence of an adequate response, a Notice of Objection.

A similar provision enables the BMA to issue such notices where it has reached adverse conclusions, on the same criteria, against an existing shareholder controller.

The Act provides for consequences for failing to provide the BMA with the level of notice in respect of the acquisition of shares in question or continuing to be a shareholder controller after receiving a Notice of Objection. In such cases a further notice will be served to direct one or more of the following restrictions:

1. Prohibiting any transfer or agreement to transfer the shares in question;
2. No voting rights shall be exercisable in respect of the shares in question;
3. No further shares shall be issued in right of the shares in question or pursuant to any offer made to the holder; and
4. No payments be made of any sum owed from the institution on the shares, except on liquidation.

The Act further provides that the Court may, on application of the BMA, order that the shares be sold. No application can be made until the expiry of the Appeal period in respect of the Notice of Objection. The proceeds of sale are to be paid into the Court for the benefit of the person beneficially interested in them.

Digital Asset Business

Bermuda has really embraced the digital asset and Fintech space, however, there still remains a lot of uncertainty in the public realm, and this is no doubt somewhat related to the pace at which the digital asset space is evolving. What are some of the risks that arise in the digital asset space and how are they changing?

The risks linked to digital assets are definitely evolving. While solutions have emerged to mitigate the early risks associated with digital assets like ML/TF, theft, etc., some new risks are emerging as the technology becomes more streamlined. For example, concerns around governance, financial stability, liquidity, pricing, etc. Our regulatory framework is fit for the evolution of these risks as the digital asset market matures.

One of the key concerns arising is that the identity of the individuals behind a digital asset is hard to identify. What is the BMA doing to ensure that CDD on applicants is valid and complete when you review digital asset business applications?

Prior to the licensing of a digital asset business (DAB), all applicants must undergo a thorough application and screening process. The Authority's expectations for applications are no different for digital assets business than for other licensed business activity.

As noted in the BMA's guidance on DAB applications, information on the DAB applicant's corporate shareholders and ultimate beneficial owners must be provided to the BMA on personal declaration forms.

At the incorporation stage, the Authority looks through any corporate veil to the ultimate beneficial owners and requires information on direct, intermediate and ultimate ownership at the incorporation stage.

At the licensing stage, the prudential and AML/ATF teams use detailed application forms, personal and institutional questionnaires to obtain information and vet shareholder controllers, directors and officers and may use regulator-to-regulator requests as part of their fit and proper screening and vetting processes prior to licensing.

Furthermore, all digital asset businesses are required to comply with Bermuda's AML/ATF regulations, including those that pertain to CDD and sanctions screening.

We understand that the BMA has reviewed some digital asset business applications to date, what are the most common deficiencies identified within the applications?

When reviewing applications, we are really looking for entities that understand the risks they are facing. This risk analysis is then expected to trickle down to each aspect of their business.

The first area of emphasis is AML/ATF. Of course it is very important to maintain the reputation of Bermuda – but also several of these companies are coming from overseas and do not necessarily understand all the intricacies of our AML/ATF framework.

The second area of emphasis is cyber security – as data becomes money, DABs need to ensure the data is well protected.

The cybersecurity programme should be risk based, protect the data and the systems, detect intrusions and breaches, respond to events, and ensure proper recovery in case of disruption.

Subsequent to the BMA's review of DAB applications, and once an applicant has been licensed to conduct DAB, what is the prudential supervisory approach?

The supervision arsenal is similar to other sectors like insurance but we have the added benefit of receiving transaction data from entities and to be able to use open blockchain data as well.

The BMA has entered into an agreement with a blockchain forensic service provider and will layer its own data on top to supervise transactions, get alerts and, at some point, evaluate prudential risks. Of course, human to human supervision is still a very effective tool so we will be conducting onsite inspections, offsite inspections and be in frequent contact with the licensees.

Also, there are two types of licenses available. The F license, for full license, and the M license, for a modified license. The latter gives the Authority more flexibility around some of the requirements but are limited in time and in scope. The added flexibility comes with increased supervision and the BMA generally plan to hold monthly review meetings with holders of M licenses.

A consistent theme is that it seems that non-digital RFIs are struggling to maintain compliance with the ever-changing legislation which provide new aspects and standards regularly. Is trying to build, supervise and regulate a new market, with many unknown risks, setting the jurisdiction up for failure?

We are a lot more protected as a jurisdiction when there is a proper regulatory and supervision framework in place – like the DAB framework. The recent case of Quadriga, a Canadian cryptocurrency exchange which lost $135 million when its founder died suddenly, exemplifies a failure in corporate governance. Corporate governance is a key requirement in Bermuda under the DAB legislation.

Moreover, as it relates to maintaining compliance, considering the digital nature of these entities, they have the ability to build new systems that don't have to deal with legacy infrastructure. This flexibility combined with the transparency of public blockchains provide for a new level of regulatory supervision.

Does the BMA plan to provide specific guidance on the controls and processes of how digital asset business should be handled in accordance with AML/ATF regulatory requirements?

The Authority has published, to complement the existing AML/ATF framework, sector specific guidance notes for DAB. They are available on the BMA website. Of course, the BMA remains available to discuss any unclear matter either on the phone or in person.

For DABs, how can individuals be sufficiently vetted if they are young and part of a start-up company?

DABs are not necessarily start-ups, and will likely involve someone with previous experience in a finance company, a tech company or both. There are also tools available for comprehensive screening of individuals. These may be particularly effective for individuals with a history in the tech business, or anyone who is particularly active online. These individuals are likely to have a large "online footprint" which can reveal a lot of information about them.

Glossary

AML: Anti-money laundering
ATF: Anti-terrorist financing
BMA: Bermuda Monetary Authority
CDD: Customer due diligence
CFATF: Caribbean Financial Action Task Force
CPI: Corruption Perceptions Index
CSP: Corporate Service Provider
DAB: Digital asset business
EDD: Enhanced due diligence
EU: European Union
FATF: Financial Action Task Force
FIA: Financial Intelligence Agency
GN: Guidance Notes for AML/ATF RFIs on AML/ATF 2016
INCSR: International Narcotics Control Strategy Report
ME: Mutual Evaluation
ML: Money laundering
MLRO: Money Laundering Reporting Officer
NAMLC: National Anti-Money Laundering Committee
NED: Non-executive Director
PEP: Politically Exposed Person
RFI: Regulated Financial Institution
SAR: Suspicious activity report
SoF: Source of Funds
SoW: Source of Wealth
TF: Terrorist financing
TSP: Trust Service Provider

Contact us

Charles Thresh
Managing Director
+1 441 294 2616
charlesthresh@kpmg.bm

kpmg.bm