# Cayman Monetary Regulatory Authority International

At the forefront of financial regulation, the Cayman Monetary Regulatory Authority International (CMRAI) is dedicated to upholding the highest standards of financial oversight and compliance. Our mission is to safeguard the stability and integrity of the global financial system by ensuring that financial services operate within a framework of transparency, accountability, and excellence.

As a trusted partner to financial institutions worldwide, CMRAI provides rigorous supervision, innovative solutions, and strategic guidance to foster a secure and thriving financial environment. With decades of experience and a commitment to global standards, we stand as a pillar of trust and security in an ever-evolving financial landscape.

With a legacy of excellence in financial oversight, the Cayman Monetary Regulatory Authority International (CMRAI) is a beacon of trust in the international financial community. Our role extends beyond regulation; we are innovators, collaborators, and protectors of the global financial ecosystem. By fostering compliance, promoting best practices, and embracing technological advancements, CMRAI ensures that financial services remain resilient and adaptable in a dynamic global market.

Our comprehensive approach to regulation encompasses a deep understanding of financial risks and a proactive stance on emerging challenges. We are committed to empowering financial institutions with the tools and guidance necessary to navigate complex regulatory landscapes, thereby contributing to global economic stability and growth.

1 Cayman Monetary Regulatory Authority International SUMMARY OF PRIVATE SECTOR CONSULTATION AND FEEDBACK STATEMENT 2020 AMENDMENTS TO THE GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS OF DECEMBER 13, 2017 ONGOING MONITORING Section Industry comment Authority s response Consequent amendments to the draft GN C. International Framework 2. FSPs should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of ML or TF are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Increasing the degree and nature of monitoring of the business relationship could be very difficult to implement as most large FSPs utilize automated monitoring systems which may not be possible to amend the degree and nature of monitoring. The Authority is of the view that enhanced CDD measures consists of more than automated monitoring. Effective monitoring systems should possess the ability to be adjusted to monitor risks. Additional methods of enhanced CDD can also be utilized. None 2 E. Obligations of FSPs 3. Policies and procedures must document appropriate measures for ensuring that data or information collected during the customer s onboarding process are kept up-to- date and relevant by undertaking routine reviews of existing records. This does not mean that there needs to be automatic renewal of expired identification documents (e.g. passports) where there is sufficient information to indicate that the identification of the customer can readily be verified by other means. The reference to can readily be verified by other means. has featured in the GNs since the 2017 revisions (or possibly earlier) and has caused confusion. In prior conversations, CMRAI has indicated verbally that this does not mean there needs to be other identification documentation on file other than a passport but the above reference could be interpreted differently depending on the examiner. We would suggest that this is amended. We believe the intent here is to say that there is no need to automatically renew expired identification documents where the FSP is satisfied with the identification of the customer, or something along those lines. The Authority expects that the ongoing monitoring obligations of FSPs as set out in the AMLRs are adhered to and as such, simply updating previously submitted onboarding documentation, is not by itself considered a sufficient risk mitigant. None We recommend rewording the first sentence to: Policies and procedures must document appropriate risk-based measures for ensuring that data ... Noted. Amended 3 12. It is expected that transactions monitoring and transactions processing are carried out by separate functions, to minimize any possible conflicts of interest. We recommend rewording this paragraph to read: Depending on the transactions processing risk of the FSP, it is expected that transactions monitoring and transactions processing are carried out by separate functions, to minimize any possible conflicts of interest. The Authority s expectations are that the transactions monitoring and transactions processing are separate functions. None 16. The transactions monitoring programme for FSPs should provide for the identification of possible trigger events and how they should be interpreted. Potential trigger events

which FSPs could consider including the following: ... (6) Customer requesting new of higher risk product. While a higher risk product is something that will be considered when assessing the risk of a customer, we suggest that the fact that a client is requesting a new product is not something that standing alone, would trigger an event driven review unless such product would result in a change in the customer risk rating. As such, we recommend the following for subparagraph (6): Customer requesting a higher risk product that would result in a change in the customer s risk. The trigger events listed are examples only. Trigger events may constitute a combination of several factors. Additionally, a single change in product request may not theoretically result in a customer risk profile change. None 4 17. Based on their own assessment, FSPs should conduct a review of all trigger events associated with its customers. While examples of trigger events should be provided to staff, training should also be delivered in order to inform staff how to identify new and emerging trigger events. FSPs should beware that compiling a definitive list of trigger events is a non-risk-based mechanism which could result in an inadequate customer monitoring process. We recommend deleting ... training should also be delivered in order to inform... and inserting ... should be aware... The paragraph should read: Based on their own assessment, FSPs should conduct a review of all trigger events associated with its customers. While examples of trigger events should be provided to staff, staff should be aware how to identify new and emerging trigger events. FSPs should beware that compiling a definitive list of trigger events is a non-risk- based mechanism which could result in an inadequate customer monitoring process. The Authority expects staff be trained to identify trigger events. None 20. Where an FSP s customer base is homogenous, and where the products and services provided to customers result in uniform patterns of transactions or activities, e.g. deposit-taking activity, it will be more straightforward to establish parameters to identify unusual transactions/activities. However, where each customer is unique, and where the product or service provided is bespoke, e.g. acting as trustee of an express trust, an FSP will need to tailor their monitoring systems to the nature of its business and facilitate the We recommend removal of the word systems from the second sentence. Noted. Amended 5 application of additional judgement and experience to the recognition of unusual transactions/activities. 22. FSPs should consider implementing transactions monitoring systems commensurate with the size, nature and complexity of its business, whether automated or otherwise. If an FSP implements a system that is partially or fully automated, then they should understand its operating rules, they should perform integrity verification on a regular basis and ensure that it addresses the identified ML/TF/PF or sanctions-related breaches. FSPs are responsible for the quality of all outputs from any automated system, including those from third-party vendors. We recommend amending the first sentence to read: FSPs should implement a risk-based transactions monitoring commensurate with the size, nature and complexity of its business, whether automated or otherwise. Noted Amended N/A We recommend a statement in this section which expressly cross-refers to the Guidance Notes Amendments December 2018 and the ability documented therein to "rely" on service providers for AML CFT P&P. This new statement should make it clear that reliance upon such P&P may be used by RFBs to meet the new ongoing monitoring requirements too. In the investment fund industry, the fund may not have personnel and may (as permitted already) rely on The Authority is of the opinion that the

Guidance Notes (Amendment), 2018 sufficiently captures the reliance and delegation scenarios specific to mutual funds and mutual funds administrators and there is no need to cross-reference the ongoing monitoring section of the GN. None 6 the P&P of its administrator it should be made expressly clear that it is acceptable for funds to rely on such administrator / service provider's P&P to meet the ongoing monitoring requirements. There is clearly no intention that funds which already use the "reliance" option would need a separate and standalone "ongoing monitoring" policy themselves. 25. The frequency of ongoing monitoring for any customer should be determined by the level of risk associated with the relationship. Having assigned a lower ML/TF/PF risk classification based on identification and verification of a customer should not be the basis of conducting a low level of ongoing monitoring. The application of SDD to low risk customers does not exempt FSPs from the obligation to conduct ongoing monitoring or from their duty to report suspicious activities to the FRA. Where FSPs have applied SDD in case of low risk scenarios, FSPs may choose to adjust the extent of ongoing monitoring of the business relationship commensurate with the low risks. Where ML, TF and PF risks are high, FSPs should apply enhanced monitoring, increasing the frequency and intensity. We recommend amending the paragraph to include the sentence in bold: The frequency of ongoing monitoring for any customer should be determined by the level of risk associated with the relationship . It should be noted that ongoing monitoring is separate to the completion of a periodic review.... We recommend deleting the following as it appears to contradict the intent of the paragraph: ...Having assigned a lower ML/TF/PF risk classification based on identification and verification of a customer The expectations for a periodic review is discussed in other areas of this section of the GN and thus it should be clear to FSPs that this is a separate process from ongoing monitoring. The Authority will delete Having assigned a lower ML/TF/PF risk classification based on identification and verification of a customer should not be the basis of conducting a low level of ongoing monitoring. The paragraph will now read: The frequency of ongoing monitoring for any customer should be determined by the level of risk associated with the relationship. The Amended 7 should not be the basis of conducting a low level of ongoing monitoring. application of SDD to low risk customers does not exempt FSPs from the obligation to conduct ongoing monitoring or from their duty to report suspicious activities to the FRA. Where FSPs have applied SDD in case of low risk scenarios, FSPs may choose to adjust the extent of ongoing monitoring of the business relationship commensurate with the low risks. Where ML, TF and PF risks are high, FSPs should apply enhanced monitoring, increasing the frequency and intensity. For more guidance on the identification and assessment of risks, FSPs should refer to Section 3 (C) of Part II of these Guidance Notes. 28. FSPs should demonstrate a periodic review of all customers, the frequency of which is decided by the FSP and based on the level of ML/TF/PF or sanctions-related risks associated with the customer. Therefore, FSPs are expected to adjust the level of ongoing monitoring in line with their institutional risk assessment and individual customer risk profiles. We believe this should be risk-based and as such should read: FSPs should demonstrate a periodic review of customers, the frequency of which is decided ... The Authority expects the periodic review timeframe and methodology will be determined by the FSP but will consist of a review of all customers. None 8 Staff with responsibility

for this function should be provided with training on how to carry out such a review. We recommend amending this paragraph as the control is the actual review being completed effectively as opposed to FSPs having to obtain evidence of training. The paragraph should read: Staff with responsibility for this function should be aware of how to carry out such a review. The Authority expects FSPs to be able to demonstrate that staff have been trained to carry out such reviews. None