GUIDANCE NOTES (AMENDMENTS) ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

Issued by the Cayman Islands Monetary Authority
Pursuant to section 34 of the Monetary Authority Law (2020 Revision)

These Guidance Notes amend the Guidance Notes issued on December 13, 2017
(the "GN of December 13, 2017")

February 2020

This document is intended to provide general guidance to Financial Service Providers ("FSPs"). It should therefore, not be relied upon as a source of law. Reference for that purpose should be made to the appropriate statutory provisions. However, FSPs should be aware of the enforcement powers of the Supervisory Authorities under the Anti-Money Laundering Regulations (2020 Revision) ("AMLRs") and amendments thereto as they relate to supervisory or regulatory guidance.

Contact:
Cayman Islands Monetary Authority
171 Elgin Avenue, SIX, Cricket Square
P.O. Box 10052
Grand Cayman KY1-1001
Cayman Islands

Tel: 345-949-7089
Fax: 345-945-6131

Website: www.cima.ky
Email: CIMA@cima.ky

1. These Guidance Notes may be cited as the **Guidance Notes (Amendment) (No.4), February 2020**.

2. The GNs of December 13, 2017 are amended to repeal Subsection **H**, Section 4 in **Part II**.

3. The GNs of December 13, 2017 are amended to include Section 16 in **Part II**, as follows:

Section 16

ONGOING MONITORING

A. APPLICABILITY

1. This section of the Guidance Notes applies to all persons conducting relevant financial business in the Cayman Islands.

B. OVERVIEW OF ONGOING MONITORING

1. Financial services providers ("FSPs") are required to understand the purpose and intended nature of the business relationship which it has with a customer. FSPs shall assess and ensure that the nature and purpose of the business relationship is in line with its expectation of the customer, and this information should form the basis for ongoing monitoring. Conducting ongoing monitoring is essential for FSPs to maintain understanding of a customer and the business relationship, keep the CDD documents up-to-date, review and revise risk assessments as appropriate, and identify unusual transactions and activities and report.

2. Pursuant to its obligations under the Anti-Money Laundering Regulations ("AMLRs"), an FSP is required to conduct ongoing monitoring on a business relationship to the extent reasonably warranted by the risk of money laundering, terrorist financing and proliferation financing ("ML/TF/PF") and sanctions-related risks. Ongoing monitoring includes:

   (1) Ensuring that documents, data or information collected under the customer due diligence process remains current and relevant to the customer. This is done by reviewing existing customer's records based on their assigned level of risk, and/or based on a change in their profile; and

   (2) Reviewing of transactions conducted to ensure that they are consistent with the FSP's knowledge of the customer, which may include the customer's source of funds and source of wealth, along with the customer's occupation and/or business.

3. Ongoing monitoring is not a customer-driven rule, but rather a transaction-driven rule. Failure to adequately monitor for activity occurring within FSPs because such monitoring is done solely on account or direct customer basis may put FSPs at risk for AML/CFT deficiencies.

4. FSPs are obligated to monitor transactions occurring by at or through them. Figure 1 summarises the cycle for ongoing monitoring, which forms part of the Authority's expectations for the AML/CFT compliance programmes of FSPs.

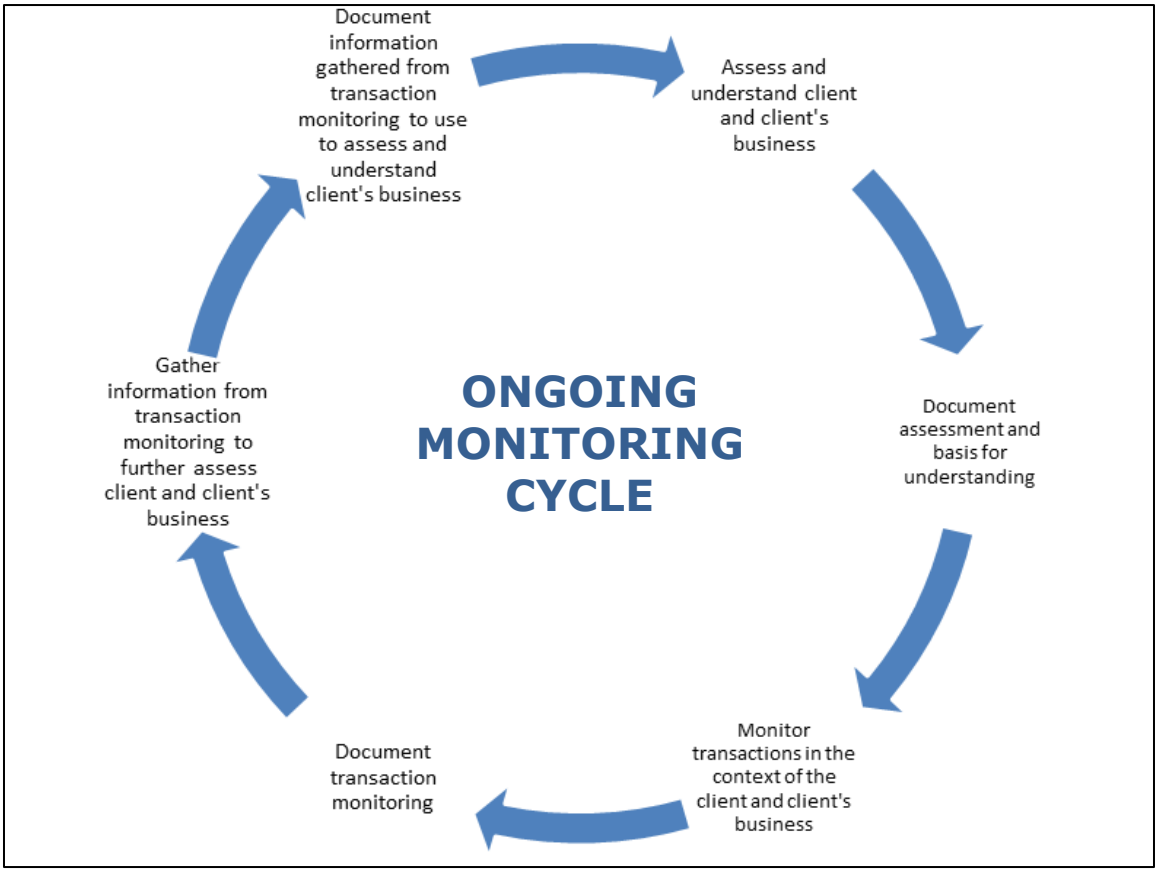

Figure 1: Process for Ongoing Monitoring

C. INTERNATIONAL FRAMEWORK

1. Recommendation 10 of the Financial Action Task Force's ("FATF") 40 Recommendations highlights that financial institutions should be required to ensure that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers[1].

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[1].

[1] Financial Action Task Force. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. (June 2019)

D. DOMESTIC LEGISLATION

1. The AMLRs (as amended) outline the requirements of a person carrying out relevant financial business to implement procedures and systems to scrutinise transactions and review customer documentation with the aim to prevent money laundering, terrorist financing, proliferation financing and sanctions-related breaches.

2. These requirements are set out in Regulations 5 and 12 of the AMLRs (as amended).

E. OBLIGATIONS OF FSPs

1. FSPs must develop and apply written policies and procedures relating to ongoing monitoring as part of their AML/CFT compliance programme.

2. The risks associated with ML, TF and PF are different, therefore FSPs are expected to put in place measures tailored to each of these risks. As an example, ML risk may be increased with unusual large transactions, while TF or PF risks are increased with unusual small transactions in targeted jurisdictions.

Reviewing Customer Information

3. Policies and procedures must document appropriate risk-based 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.

4. The intentions of the customer, nature and risk of the transactions and business relationships should determine the documentation maintained as part of the FSP's records. Particular attention should be paid to higher risk categories of customers and their business relationships.

5. FSPs must assess the information received as a part of ongoing monitoring to determine whether it affects the risk associated with the business relationship. Where the basis of a relationship has changed, FSPs must re-evaluate the risk rating of the customer. Also, FSPs must carry out further CDD procedures to ensure that the revised risk rating and basis of the relationship is fully understood. Ongoing monitoring procedures must take into account changes in the customer's risk. If the risk changes significantly, then enhanced due diligence ("EDD") or simplified due diligence ("SDD") should be applied[2].

6. As part of its periodic reviews, an FSP is required to update the CDD records as determined by the customer's assigned level of risk or on the occurrence of a triggering event (see paragraph 16 of this subsection), whichever is earlier.

7. If an FSP has a suspicion of ML, TF, PF or sanction-related breaches, then the FSP is required to make the relevant disclosures to the competent authority.

[2] FSPs may conduct SDD in case of lower risks identified, while EDD must be applied where higher risks are identified.

8. FSPs must ensure that its customers are periodically screened against required sanctions lists (see the section on Targeted Financial Sanctions) as a part of their ongoing monitoring and periodic review processes, in order to identify and freeze assets of and report designated persons to the relevant authorities without delay.

9. Policies and procedures must clearly outline the remedial action required when the required CDD documentation or information is not held on file, including the various steps that should be taken to locate or obtain such documentation or information.

Transactions Monitoring

10. FSPs must be able to identify the transactions/activities of customers during the course of the business relationship, that is, the anticipated type, volume and value of transactions/activities. The aim is to ensure that transactions/activities are consistent with the FSPs' knowledge of the customer, the customer risk assessment, and the purpose and intended nature of the business relationship.

11. Ongoing monitoring of transactions is an essential component, which aids in identifying transactions/activities that are unusual or potentially suspicious, therefore FSPs are to ensure that they have a robust process in place to monitor transaction activities. The intention is to reduce the possibility of the occurrence of ML/TF/PF or sanctions breach without detection and to meet the obligations set out in the AMLRs.

12. It is expected that transactions monitoring and transactions processing are carried out by separate functions, to minimise any possible conflicts of interest.

13. It is recognised that the most effective method of monitoring of accounts is achieved through a combination of automated and manual solutions. It is important to note that a culture of compliance coupled with well-trained, vigilant staff aid in forming an effective monitoring system overall.

14. An FSP's transactions monitoring process should be well-documented and subjected to regular reviews including assurance testing, to ensure their process is functioning adequately in identifying any potential suspicious ML/TF/PF activities or sanctions-related breaches.

15. FSPs must be vigilant for changes in the nature of the relationship with the customer over time.

Trigger Events

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 include the following:
    (1) A material change in ownership and/or management structure;
    (2) Reclassification of the jurisdiction, where the customer or respondent institution is based;
    (3) The identification or entry of a politically exposed person ("PEP") in the business relationship;
    (4) Inconsistencies between customer information and supporting verification evidence;
    (5) Identification of adverse information from sources such as media reports or other relevant sources; or

(6) Customer requesting a new or higher risk product.

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 transaction monitoring process.

Unusual Transactions (refer also to Section 9 of Part II of the GNs)

18. FSPs should have adequate policies and procedures to identify unusual transactions. These transactions may include:
    (1) Transactions that are inconsistent with customer profile;
    (2) Transactions that do not follow the same pattern compared with the customer's normal activity or that of a similar customer, products or services;
    (3) Transactions where the FSP is not aware of a reason or lawful purpose or doubts the validity of the information submitted.

19. FSPs should be able to identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely manner.

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 to the nature of its business and facilitate the application of additional judgement and experience to the recognition of unusual transactions/activities.

21. Where an alert has been generated, either by an automated system or a manual review of the customer file, FSPs should attempt to establish the reason for changes in behaviour and take appropriate measures, such as conducting additional CDD and if warranted, submitting the relevant disclosures to the Financial Reporting Authority ("FRA"), such as an suspicious activity report ("SAR"), an Asset Freeze Report or a report regarding the transactions attempts by a designated person.

Monitoring Systems

22. FSPs should consider implementing a risk-based 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.

23. Transactions monitoring systems should be reviewed regularly to ensure that that the systems are operating appropriately and effectively. Furthermore, they should be reviewed to accommodate changes for emerging risks, new trends and regulations.

24. Examples of the types of monitoring systems FSPs should put in place may include:
    (1) Transaction monitoring systems that detect anomalies or suspicious patterns of behaviour, including the unexpected use of a product in a way for which it was not designed;
    (2) Systems that identify discrepancies between submitted and detected information, for example, between submitted country of origin information and the electronically detected IP address;
    (3) Systems that compare data submitted with data held on other business relationships and that can identify patterns such as the same funding instrument or the same contact details;
    (4) Systems that identify whether the product is used with merchants dealing in goods and services that are associated with a high risk of financial crime and/or sanctioned entity.

Frequency of Review

25. The frequency of ongoing monitoring for any customer should be determined by the level of risk associated with the business relationship. 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. For more guidance on the identification and assessment of risks, FSPs should refer to Section 3 of Part II of these Guidance Notes.

26. When assessing CDD obligations in relation to the ongoing monitoring of customers, FSPs should ensure that they have effective and relevant ongoing monitoring policies and procedures in place, which are adhered to by all staff.

27. FSPs should have a well-documented and efficient ongoing monitoring programme in place, which demonstrates a risk-based approach where higher risk customers are reviewed on a more frequent basis.

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. Staff with responsibility for this function should be provided with training on how to carry out such a review.