GIBRALTAR FINANCIAL SERVICES COMMISSION

6. Ongoing Monitoring

GFSC AML/CFT/CPF Guidance Notes

Table of Contents

6.1 Ongoing Monitoring

AML/CFT/CPF Requirements

R19 A regulated entity must have adequate systems and controls in place to enable the scrutiny of transactions undertaken throughout the course of a business relationship, to ensure that those transactions are consistent with:

a) The nature and purpose of the business relationship;
b) The regulated entity's knowledge of the customer;
c) The risk profile of the customer; and
d) The economic profile of the customer (including, where relevant, the source of funds and wealth).

R20 A regulated entity must apply a risk-based approach to the review of its existing records relating to each business relationship (and update these where necessary) to ensure that the risk profile of each customer and the data or information obtained for the purposes of customer due diligence, are kept up-to-date and relevant.

Guidance

1. The application of customer due diligence measures is not considered to be a one-off exercise to be carried out solely prior to the establishment of a business relationship or occasional transaction. To continuously ensure the effectiveness and appropriateness of these measures as a business relationship progresses, regulated entities must continue to monitor each business relationship throughout the duration of that relationship[1].

2. Effective ongoing monitoring of a business relationship consists of the following distinct aspects:
   a) The scrutiny of transactions undertaken throughout the course of the relationship[2]; and
   b) Periodically reviewing and updating existing due diligence and risk assessment records on a risk-sensitive basis to ensure that they are accurate and kept up-to-date[3].

3. The application of ongoing monitoring measures allows a regulated entity to remain abreast of any changes in circumstances to its customers. The regulated entity is also able to certify the robustness of its understanding of each business relationship and ultimately identify any activity by a customer which may be considered suspicious or illicit.

4. In all instances, it is imperative that all staff members involved in the application of an entity's AML/CFT/CPF controls (or otherwise forming part of the review of transactional/user information) remain aware of the potential red flags and typologies associated with an entity's customer base as this may be indicative of suspicious activity. This should be a key focus of each regulated entity's staff training plans. For further guidance on requirements relating to training, please refer to the "Training" section of these Guidance Notes.

5. In addition to the ongoing monitoring measures outlined above, a regulated entity is also required to screen the entirety of its customer base against the relevant sanction lists (i.e. the United Nations, European Union, United Kingdom & Gibraltar lists) on an ongoing basis.

[1] Section 12(1), Proceeds of Crime Act 2015
[2] Section 12(2)(a), Proceeds of Crime Act 2015
[3] Section 12(2)(b), Proceeds of Crime Act 2015

Screening must be undertaken without delay[4], as and when each of the relevant sanction lists are revised or updated. For further guidance on sanction screening requirements, please refer to the "Policies, Procedures & Controls" section of these Guidance Notes.

6.2 Scrutiny of Transactions

6.2.1 Identification of Suspicious or Unusual Activity

6. Scrutiny of the transactional activity undertaken throughout the course of a business relationship plays a crucial role in the identification of suspicious activity. Depending on the nature of a regulated entity's customer base and the types of services or products being provided, each regulated entity must identify and be aware of the potential red flags and typologies associated with the activities of its clients as this may be indicative of illicit activity.

7. In order to comply with the provisions set out under Section 12(1)(a) of the Act, a regulated entity must establish and maintain appropriate procedures and controls to monitor the transactional activity of its customers. This will allow it to identify any unusual activity that should then be subject to further examination. When determining whether a customer's transactional activity is considered significant or unusual, a regulated entity must pay due regard to:
    a) Whether the transactional activity is inconsistent with the regulated entity's understanding of the business relationship (including its nature and purpose, the particulars of the customer, and the customer's economic and risk profiles);
    b) Whether the transactional activity forms part of an unusual pattern;
    c) Whether the transactional activity is considered complex or unusually large; or
    d) Whether the transactional activity is deemed to fall within the remit of a red flag or typology associated with an increased risk of ML, TF or PF.

6.2.2 Use of Transaction Monitoring Rules & Thresholds

8. It is ultimately the responsibility of each regulated entity to know its customer base to the extent that it is able to appropriately recognise and identify any suspicious transactions or activity. The assessment of transactional activity can either be conducted through a case-by-case review by an appropriate member of staff or through the development of a system to monitor rules and thresholds to trigger escalation.

9. The implementation of any rules and thresholds must be carefully considered to ensure that high risk or suspicious activity is not able to occur without identification. Prior to the implementation of a transaction monitoring rule-set (or the modification of an existing one), a regulated entity should conduct a thorough analysis to ensure the adequacy of each threshold.

10. Following the implementation of such triggers, the effectiveness of each individual rule must be assessed on an ongoing basis. Best practice would dictate that a sample of transactions is selected for review on a periodic basis to ensure that these parameters are still accurate and fit for purpose. When determining whether a particular rule or threshold should be added, removed or modified, a regulated entity should consider whether:
    a) There has been a change to the customer demographic;
    b) There has been a change to the typical transactional activity or patterns of customers;

[4] Section 8(3), Sanctions Act 2019

c) There has been a particular trend observed in the unusual or suspicious activity that has been identified; or
d) Whether a particular rule is no longer deemed necessary or appropriate.

11. When expanding operations or launching a new product/service, a regulated entity must have governance measures in place to allow for the consideration of the threats, vulnerabilities and typologies associated with that product. These considerations must also include an assessment of the appropriateness of the current transaction monitoring rule set in place (where applicable), and whether any of these rules should be amended.

6.2.3 Automated vs. Manual Monitoring

12. Depending on a number of factors, the manual review of all transactional activity may not be deemed feasible or appropriate. A regulated entity must consider whether a more appropriate option would be to implement a formal transaction monitoring solution (either developed in-house or outsourced to a third party). When determining the appropriateness of manual transaction monitoring, a regulated entity should consider:
a) The nature of the products and services offered;
b) The size and nature of the client base;
c) The volume of transactions that occur within a specified time period; and
d) The capacity of the regulated entity's staff members involved in the review of transactional activity.

13. When reviewing transactions on a manual basis, a regulated entity must pay particular care to ensure that it retains all relevant records and audit trail information evidencing the assessment of transactions undertaken by its client base.

14. The use of any third-party system constitutes an outsourcing arrangement, and as such must comply with the GFSC's Outsourcing Guidance Notes[5]. It should be noted that the implementation of a transaction monitoring system does not always eliminate the need for manual review, on the basis that at a minimum, a regulated entity's MLRO will be required to assess any potential suspicious activity and determine whether the matter should be escalated to the GFIU. The use of an automated system also does not absolve a regulated entity of the need to ensure that its staff members receive adequate training to facilitate the identification of suspicious activity and the relevant reporting requirements. For further guidance on the identification and escalation of suspicious activity, please refer to the "Suspicious Activity Reporting" section of these Guidance Notes.

Sector-Specific Guidance – Trust & Company Service Providers ("TCSPs")

15. As stated above, a regulated entity is required to scrutinise the transactional activity of its customers. A regulated entity's application of ongoing monitoring controls must be risk-based. It is therefore not expected that a regulated entity would be required to scrutinise every single transaction carried out by the customers to which it provides relevant financial business. In the case of the TCSP sector, this monitoring is typically undertaken manually. The requirement for TCSPs to apply ongoing monitoring measures, applies regardless of the type of product or service being provided. Although the GFSC recognises that transaction monitoring in cases where a TCSP does not provide directorship services may be more challenging, the requirements remain applicable. Furthermore, it may be argued that the AML/CFT/CPF risk posed increases

[5] GFSC Outsourcing Guidance Notes

where a TCSP solely provides registered office and/or secretarial services as it may have less oversight of the activities that the customer is carrying out.

16. Where the continued administration and management of the legal persons and arrangements (e.g. asset disbursements and corporate filings) would also enable a TCSP to develop a better understanding of the economic activities of its clients, there are several ways in which the firm can carry out ongoing monitoring of its customers depending on the customer's risk profile and nature of the activity (which may vary, e.g. an asset holding company, trading company, consulting company, etc.). Below is a non-exhaustive list of examples of documents which could be requested from a customer to assist in satisfying transaction monitoring requirements:
    - Bank statements;
    - Annual accounts;
    - Payment receipts;
    - Invoices;
    - Board minutes;
    - Rental agreements;
    - Contractual agreements;
    - Third party agreements; and
    - Maintenance receipts (e.g. of a property or yacht).

17. In addition to the above, it would also be expected that:
    a) A TCSP maintains client accounting records at the registered office[6]; and
    b) A TCSP which provides directorship services to its clients, will maintain minutes from Director's meetings at the registered office.

Sector-Specific Guidance – Virtual Asset Service Providers ("VASPs")

18. The immutable and public nature of the blockchain allows VASPs to assess whether a particular wallet address or set of assets has had any exposure to high risk or illicit sources (e.g. the "darknet market"). A regulated VASP must have controls in place to determine whether any identified exposure is considered to be directly associated with the customer in question and requires further action or escalation. The nature of VA exposure will often warrant carrying out a case-by-case review to determine the level of materiality between the customer and the source in question.

19. A regulated entity must ensure that its monitoring process takes into account both direct and indirect exposure to sources of illicit activity/risk. The number of "hops" (i.e. movement from one wallet address to another) away from a source of risk which is deemed to be directly related to a customer, may ultimately be subject to a case-by-case assessment made by the regulated entity in question. In cases where exposure is identified (and is deemed to not be directly related, and therefore not warranting the exiting of the client relationship or the disclosure of a SAR), a regulated entity must consider whether the exposure warrants an increase to the customer's assessed risk level.

20. The GFSC expects that, as a minimum, a regulated entity not tolerate any direct exposure to illicit sources, such as the darknet market, stolen funds, scams or sanctioned wallet addresses. The use of anonymising services, such as "tumblers" or "mixers" may also be considered prohibited, on the basis that these are typically associated with obscuring the identification of "tainted" assets associated with illicit flows or services.

[6] Regulation 46, Financial Services (Fiduciary Services) Regulations 2020

21. In addition to the use of virtual asset screening services, and in line with the requirements for all other regulated entities, a VASP must also have controls and processes in place to assess the transactional patterns of its customers in line with their economic profile.

Sector-Specific Guidance – Initial Coin Offerings ("ICOs")

22. In the case of an ICO, customers will typically engage with an entity on the basis of a one-off purchase transaction. Should a particular customer then decide to purchase additional tokens as part of a further transaction, the regulated entity must consider whether the additional purchase(s) remains consistent with its knowledge of the customer and their economic profile.

23. As part of an ICO's due diligence on a customer, it should assess any exposure that the customer's wallet address has had to sanctioned, high risk or illicit sources (as set out within the "VASPs" section above). If there is a subsequent gap in time between the application of virtual asset screening measures and the issuance of the purchased tokens themselves, a regulated entity must make sure to re-screen the customer's wallet address. This is to ensure that during that time period, the wallet address in question has not been associated with any additional exposure to sanctioned, high risk or illicit sources, and that it has not been the subject of financial sanctioning measures itself.

24. As stated within the GFSC's VASP Registration Scope Guidance Note, in cases where an ICO continues to receive passive income following a token sale as a result of sales on a secondary market, the GFSC considers it best practice for the entity to continue to apply virtual asset screening controls to identify any exposure associated with sanctioned, high risk or illicit activity[7].

6.3 Periodic Reviews

6.3.1 Application of a Risk-Based Approach

25. When providing relevant financial business to a customer, it is imperative that each regulated entity has a robust understanding of the circumstances pertaining to that customer. Over the course of a business relationship, these circumstances may be subject to change. Therefore, a regulated entity must have processes in place to periodically assess each business relationship and determine whether the risk assessment and due diligence measures that have been applied remain appropriate or otherwise require updating. This review should assess the following:

a) Whether the due diligence documentation held on file remains up-to-date and relevant;
b) Whether there has been any change to the particulars of the business relationship that require the application of additional or updated due diligence measures; and
c) Whether the overall risk score attributed to the client remains appropriate.

26. As stated under Section 12(1)(b) of the Act, the undertaking of periodic reviews of a regulated entity's customer base must be conducted on a risk-sensitive basis. In practice, this means that customers which pose a higher level of ML, TF or PF risk must be subject to more frequent (and therefore more stringent) review cycles. As an example, a low-risk customer would normally be subject to less frequent reviews than a medium risk or high risk customer. The length of a regulated entity's periodic review cycles is ultimately determined by the regulated entity itself but it must be appropriate and proportionate to the regulated entity, its sector and the level of ML, TF & PF risk posed.

[7] GFSC VASP Registration Framework Scope Guidance Note

27. In addition to periodic reviews, a regulated entity should have mechanisms in place to allow for notification of any significant changes to its customers' particulars. This would include, for example, a corporate customer undergoing a change to its ownership structure, or an individual customer changing residence to a jurisdiction of increased risk. Should such changes be notified to a regulated entity, the regulated entity should not continue the business relationship as normal pending the next upcoming periodic review. Instead, this should trigger an event-driven review surrounding the notified information. Event-driven reviews may also be triggered through a multitude of other means, including transaction monitoring measures (where the transactional activity of a client is indicative of a change to the particulars of the client), ongoing open-source checks, sanctions, PEP & adverse media screening, or other means of notification/identification.

6.3.2 Ongoing Risk Assessment

28. A regulated entity is required to assess the level of ML, TF & PF risk posed by each prospective business relationship prior to its establishment[8]. The application of a customer risk assessment allows a regulated entity to determine the level of AML/CFT/CPF controls that would be considered necessary to mitigate the level of risk posed by the business relationship. The risk, however, is likely to change in level and severity throughout the course of a business relationship. Likewise, a regulated entity's own risk appetite or customer risk assessment methodology may develop and change over time.

29. The change in circumstance at the point of review may have a significant impact on the risk profile of that customer. An increased risk profile may warrant the application of additional mitigating measures and controls. To ensure that a regulated entity's approach to each business relationship remains appropriate, it must re-consider the level of ML, TF & PF risk posed by each business relationship at the point of a periodic or event-driven review. For further guidance on assessing the level of ML, TF & PF risk posed by each customer, please refer to the "Customer Risk Assessment" section of these Guidance Notes.

[8] Section 25A, Proceeds of Crime Act 2015

GIBRALTAR FINANCIAL SERVICES COMMISSION

Published by:
Gibraltar Financial Services Commission
PO Box 940
Suite 3, Ground Floor
Atlantic Suites
Europort Avenue
Gibraltar

www.gfsc.gi