GIBRALTAR FINANCIAL SERVICES COMMISSION

5. Customer Due Diligence

GFSC AML/CFT/CPF Guidance Notes

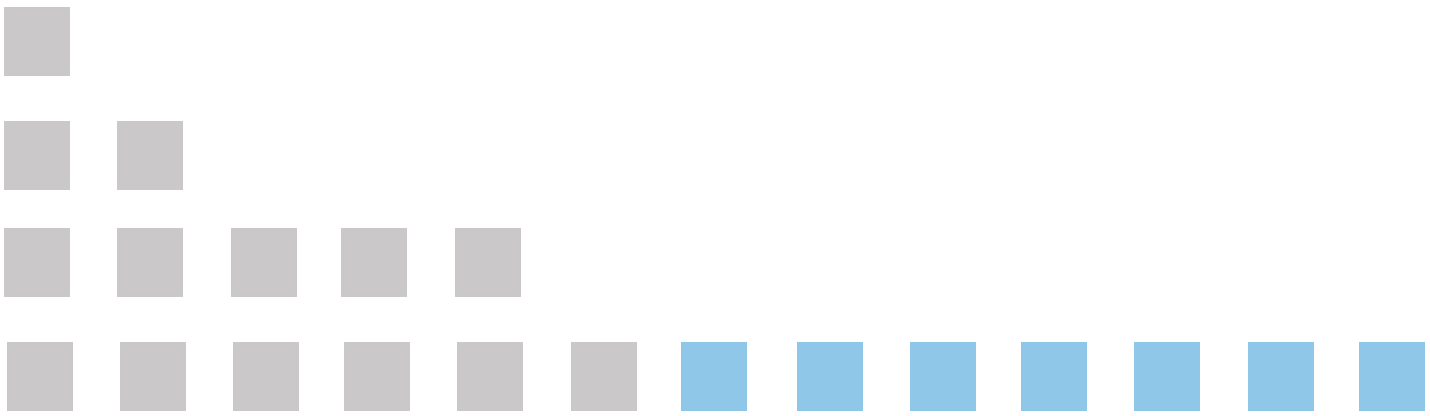


Table of Contents

5.1 Knowing Your Customer

AML /CFT/CPF Requirements

R12 A regulated entity must take appropriate measures to identify and verify the subject of a business relationship or occasional transaction. The application of these measures must be in line with the risk profile of that customer.

Guidance

1. Ensuring that there is a robust understanding of each business relationship underpins all AML/CFT/CPF-related efforts and controls and is the primary defense against a regulated entity's susceptibility to financial crime. The application of customer due diligence measures affords assurances to a regulated entity that the subject of a business relationship or occasional transaction is who they say they are. This in turn allows the regulated entity to determine whether it is appropriate to provide them with the product or service in question.

2. Section 11 of the Act requires a regulated entity to apply customer due diligence measures prior to the establishment of a business relationship or occasional transaction. These measures must be applied to the subject of the relationship/transaction, i.e. the customer and all beneficial owner(s) of the customer[1]. A regulated entity must also consider, where appropriate, whether any additional parties may also be considered to form part of the subject of the relationship/transaction, such as in the case of:
    a) Any person acting or purporting to act on behalf of the customer/beneficial owner (for example, in the case of the guardian of a natural person, an authorised signatory, persons to whom powers of attorney have been granted, or the directors/senior managers acting on behalf of a legal entity); or
    b) Any other person who is acting on behalf of the customer/beneficial owner.

3. As set out under the Act, the application of customer due diligence measures includes understanding "the purpose and nature of the business relationship or occasional transaction"[2]. In order to truly understand the proposed relationship to be held with a prospective customer, a regulated entity must have a robust awareness of the purpose for which that customer has decided to engage with the entity and its product offering. When afforded sufficient context, the purpose of a business relationship may have a significant impact on the perceived level of risk posed by a customer or may lead a regulated entity to determine that it no longer wishes to continue establishing the business relationship or carrying out the occasional transaction.

4. In order to fully know a customer and understand the purpose and nature of a business relationship, a regulated entity must ensure that that customer is not subject to financial sanctions. This is achieved through screening each customer against the applicable sanctions lists[3]. In Gibraltar, the following sanctions lists apply directly under the Sanctions Act 2019[4]:
    - United Nations;
    - European Union;
    - United Kingdom; and
    - Gibraltar.

[1] Section 10, Proceeds of Crime Act 2015
[2] Section 10(d), Proceeds of Crime Act 2015
[3] Section 8(3), Sanctions Act 2019
[4] Section 6(2), Sanctions Act 2019

5. For further guidance on sanctions screening requirements, please refer to the "Policies, Procedures & Controls" section of these Guidance Notes.

6. Failing to gather information about the purpose and nature of a business relationship or occasional transaction based on the type of transaction or product/service in question, may expose a regulated entity to undue levels of risk. In cases of potential ambiguity, a regulated entity should consider collecting further information or employing specific measures to ensure that a full understanding is achieved and documented.

5.2 Risk-Based Approach to Due Diligence

7. The identity of the customer, including the beneficial owner(s), must always be verified to some extent. The application of customer due diligence measures must be risk-based, meaning that the extent of verification required should be determined by the level of ML, TF and PF risk posed by the customer[5]. A robust assessment of the level of risk posed by a prospective customer will allow a regulated entity to determine whether it is appropriate to, for example, apply simplified due diligence measures, or conversely, whether enhanced due diligence may be required. For further guidance on the assessment of the ML, TF & PF risks posed by prospective customers, please refer to the "Customer Risk Assessment" section of these Guidance Notes.

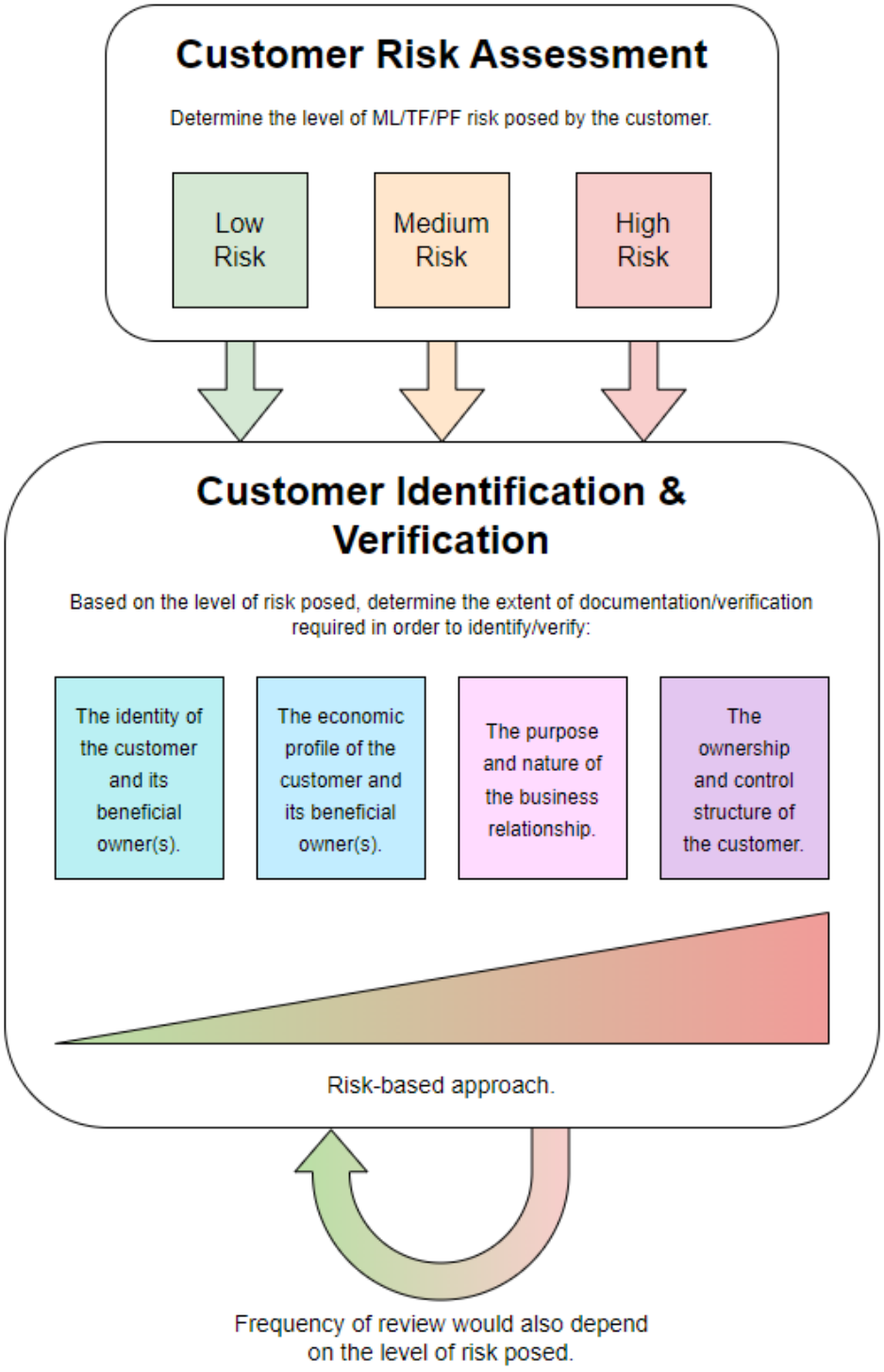
8. There is no prescriptive approach to the application of due diligence measures and controls. In assessing the risk of each prospective customer, a regulated entity must determine the appropriate level of documentation/verification required. In practice, these measures should ensure that the regulated entity identifies and verifies, on a risk sensitive basis:
    a) The identity of the customer (and its beneficial owners);
    b) The ownership and control structure of the customer (in the case of corporates and legal entities);
    c) The economic profile of the customer (and its beneficial owners); and
    d) The purpose and nature of the business relationship.

9. Following the initial on-boarding of a new business relationship, a regulated entity must continue to consider, on an ongoing basis, whether any additional identification/verification measures are necessary. Where there are any changes in circumstances associated with a customer, this may prompt a regulated entity to apply additional due diligence measures in line with any perceived increased risks. The frequency at which the risk profile of a customer (and by extension, the appropriateness of the identification/verification measures applied to date) are reviewed on an ongoing basis, should be determined by the customer's risk profile.

10. Figure 1 below visually demonstrates the relationship between the customer risk assessment and the application of a risk-based approach to due diligence measures.

[5] Section 10(e), Proceeds of Crime Act 2015

Figure 1 – The application of a risk-based approach to customer due diligence measures.



5.3 Timing of Verification

AML/CFT/CPF Requirements

R13 A regulated entity must apply customer due diligence measures prior to the establishment of a business relationship or occasional transaction[6].

Guidance

[6] Section 13, Proceeds of Crime Act 2015

5.3.1 Linked Transactions

11. In order to understand a customer and assess the level of ML, TF & PF risk posed by that customer, a regulated entity must apply customer due diligence measures prior to the establishment of a business relationship or completing an occasional transaction. With regards to occasional transactions, verification of identity is not required in the case of any transactions (whether single or linked) that are:
    a) Below 15,000 EUR[7];
    b) In the case of persons trading in goods whose transactions are carried out in cash, below 10,000 EUR[8]; and/or
    c) In the case of transactions involving virtual assets, below 1,000 EUR[9].

12. Where multiple small transactions are made by the same party (and are therefore linked), a regulated entity must pay due regard to whether the total sum of the transactions is set to breach any of the thresholds referenced above. If so, the regulated entity must apply customer due diligence measures in line with the assessed risk profile of that customer prior to carrying out the occasional transaction.

5.3.2 Identification of Beneficiaries Post-Establishment of a Business Relationship

Sector-Specific Guidance – Life Assurance Providers & Insolveny Practitioners

13. There may be exceptional cases where a regulated entity is unable to identify and verify the beneficiary of a business relationship at the point of establishment, for example, beneficiaries of life assurance and other investment-related insurance policies. In such cases, the provider in question would be required to verify the identity of the beneficiaries at the point of pay-out[10]. In doing so, the regulated entity must pay due regard to:
    a) Any additional ML, TF, PF risks posed by the beneficiaries; and
    b) Ensuring that the beneficiaries are not named terrorists, or subject to any sanctions designations at the point of pay-out.

Sector-Specific Guidance – Insolveny Practitioners

14. In the case of insolvency practitioners, where due diligence measures are unable to be completed prior to initiation of the business relationship (such as where an appointment is made at a Decision Procedure or by Court Order), reliance may be placed, in part, on the order of the appointment by the Court. Nevertheless, the insolvency practitioner must complete the appropriate level of due diligence as soon as possible. It is expected that the due diligence process would be commenced no later than five working days following the date of appointment.

5.4 Natural Persons

Guidance

5.4.1 Beneficial Ownership of Natural Persons

15. In the case of natural persons, the Act defines beneficial ownership as[11] follows:

[7] Section 11(1)(b), Proceeds of Crime Act 2015
[8] Section 11(1)(ba), Proceeds of Crime Act 2015
[9] Section 11(1)(g), Proceeds of Crime Act 2015
[10] Section 13(3), Proceeds of Crime Act 2015
[11] Section 7(1A)(a), Proceeds of Crime Act 2015

a) Where a person is conducting a transaction or activity on his own behalf, the natural person; or
b) Where a transaction or activity is being conducted on behalf of another person, the person on whose behalf the transaction or activity is being conducted.

16. When engaging with business relationships or occasional transactions with natural persons, a regulated entity must ensure that it has identified all relevant subjects, in line with the provisions set out above.

5.4.2 Application of Identity Verification Measures

17. It is ultimately the responsibility of a regulated entity to determine what verification measures should be applied to its customers based on the level of risk posed. A regulated entity must maintain an appropriate audit trail documenting its assessment of the approach taken in each case of customer identification.

18. In order to verify the physical identity of an individual, a regulated entity is typically expected to request an official identification document, such as those included within the following non-exhaustive list:
    - A passport, bearing a photograph of the natural person;
    - A national identity card (or equivalent), bearing the photograph of the natural person; or
    - A driving licence, bearing a photograph of the natural person.

19. The residence of an individual may have a significant impact on the level of ML, TF or PF risk that they pose. Aside from instances where simplified due diligence measures are able to be applied, a regulated entity is typically expected to request additional documentation to verify the residential address of their customers. The following are non-exhaustive examples of potential documentation that can be used to verify an individual's residential address:
    - A recent bank statement;
    - A recent utility bill;
    - A tenancy agreement; or
    - Copies of correspondence with an independent source.

20. There is a wide range of documentation which may be provided to verify a customer's identity or residential address. Each regulated entity must determine the appropriateness of any given document in light of its documented risk mitigation procedures and controls. Particular care should be afforded in accepting documents that are particularly susceptible to forgery or which can be easily obtained using a falsified identity.

5.4.3 Face-to-face vs. Non-face-to-face Interactions

21. In cases where a business relationship or occasional transaction has been established on a face-to-face basis, a regulated entity will be able to itself check whether the likeness of the individual is in accordance with the photograph included within the submitted identity document. In the case of non-face-to-face business relationships, a regulated entity is unable to rely on any pre-identified knowledge on the likeness of the individual, therefore, increasing the interface risk posed by the business relationship.

22. Any mechanism through which a customer interacts with a regulated entity on a non-face-to-face manner increases the regulated entity's exposure to risk. As an example, this may lead to the potential obfuscation of the true subject of a business relationship/transaction through the provision of falsified identification documentation. Additional risk mitigation controls are

therefore required to ensure adequate verification of the customer's identity. These controls may include those provided within the following non-exhaustive list:

- Requesting additional verifying documents, data or information;
- Requesting a live image or "selfie" of the individual to assess their likeness against the submitted identity document;
- Requesting the certification of identity documents, asserting whether the photograph is a true likeness of the individual in question;
- Ensuring that the first payment received in respect of that business relationship/transaction is conducted through an account in the customer's name within a regulated credit institution; or
- Sending information or documentation required to operate the business relationship/transaction to a physical address that has been verified.

5.4.4 Electronic Identity Verification Measures

23. The application of AML/CFT/CPF-related requirements is technologically neutral. When seeking to verify the identity of an individual, a regulated entity is able to make use of electronic means of verification, such as electronic databases and systems.

24. As stated within the "Customer Risk Assessment" section of the Guidance Notes, establishing a business relationship or occasional transaction through video call is considered to be equivalent to a face-to-face interaction. A regulated entity should, however, pay due care and diligence to the following factors when determining the suitability of a video call as a means of customer identity verification:

- The appropriateness and reliability of the video calling platform being used;
- The susceptibility of the video calling platform to any potential tampering;
- The strength of the internet connection and clarity of the image produced;
- The responsiveness of the individual to any questions posed during the video call;
- The speed and specificity of the answers received in response to any questions posed during the call;
- Whether the physical image produced is moving/speaking in accordance with the individual's voice;
- Ensuring that the individual is unable to apply a "filter" over their image to obfuscate their appearance; and
- Ensuring that the image produced is not a pre-recorded video.

25. The use of third-party identity verification systems for non-face-to-face business relationships has increased significantly in recent years. The FATF has issued its own Guidance on Digital Identity, which regulated entities may find useful when determining the suitability of such an approach[12]. Examples of common models of electronic identification used during the customer due diligence process include:

a) The use of biometric analysis to compare the likeness of a live "selfie" of an individual to their photographic identification document;
b) The use of visual and informational analysis to assess whether an identification document is fraudulent or has been tampered with; and
c) The use of IP address identification to aid in verifying the residence of an individual.

26. When considering the use of a particular solution, a regulated entity should assess the extent to which the tool in question can address or exacerbate certain ML/TF/PF-related risks, such as:

[12] FATF Guidance on Digital Identity

- ICT and security risks;
- Qualitative risks;
- Legal risks; and
- Impersonation fraud risks.

27. A regulated entity that relies on the use of external providers for the provision of such services remain ultimately responsible for meeting its ongoing obligations relating to customer due diligence. As with all outsourced relationships, the use of such providers should be assessed and conducted in line with the GFSC's Outsourcing Guidance Note[13], with sufficient consideration given to ensuring there is adequate oversight of the relationship.

28. When selecting the use of a particular provider (or changing providers), a regulated entity should conduct a thorough assessment of the appropriateness and reliability of the system, in line with the proposed use. This assessment should be formally documented. Some providers which may be deemed appropriate for some regulated entities/products, may be inappropriate for others dependent on a number of factors. As an example, the nature of a regulated entity's customer base may mean that a particular system would be unsuitable (e.g. some systems may not recognise identity documents from certain jurisdictions).

29. Examples of the types of elements to consider when selecting a particular provider for customer identification purposes include:
    - Whether the solution draws upon sufficient data points and sources;
    - Whether the solution is transparent in the way that it communicates the checks that were carried out, the sources that are used, how it determines the results, and how reliable the results are;
    - Whether the solution is appropriate given the business model of the regulated entity;
    - What level of testing has been undertaken to assess the appropriateness of the solution prior to implementation; and
    - What level and type of oversight would be considered appropriate over the solution.

5.5 Corporate Customers

AML/CFT/CPF Requirements

R14 In the case of customers which are legal entities, legal arrangements or similar (referred to collectively as "corporate entities" or "corporate customers"), a regulated entity must take appropriate measures to understand the ownership and control structure of the customer. This includes identifying and verifying (on a risk sensitive basis) the identity of all relevant ultimate beneficial owners.

Guidance

5.5.1 Identification of Ownership & Control

30. As stated above, in the case of all business relationships and occasional transactions, the subject of these include both the customer and its beneficial owner(s). Understanding the control and ownership structure of a corporate customer is crucial in identifying the true subject of each relationship/transaction. Where the complexity of an ownership structure does not have an

[13] GFSC Outsourcing Guidance Notes

obvious legitimate or transparent purpose, this may also be indicative of any potential red flags associated with the obfuscation of the true ultimate beneficial owner(s).

31. As with individual customers or natural persons, it is the responsibility of the regulated entity to determine the extent of documentation/verification required of each prospective corporate customer. The following is a non-exhaustive list of documentation which may be used to verify the identity of a corporate entity:

- The Certificate of Incorporation (or equivalent);
- The Memorandum of Articles or Incorporation (or equivalent);
- The latest Audited Financial Statements;
- The Register of Directors (or equivalent);
- The Register of Shareholders (or equivalent); and
- A Company Registry search extract.

32. There is a wide range of documentation which may be provided to verify a corporate entity's identity. A regulated entity must determine the appropriateness of any given document in light of its documented risk mitigation procedures and controls. Particular care should be afforded in accepting documents which can be easily falsified.

33. In addition to the above, in cases where the corporate entity is subject to registration of beneficial ownership information within the country of establishment, the regulated entity must collect proof of registration or an excerpt from the relevant register confirming registration[14]. In cases where the content of the register is not publicly available, the regulated entity should request documentary proof of registration from the corporate customer.

5.5.2 Beneficial Ownership of Corporate Entities

34. The term "beneficial owner" is defined under Sections 7 (1A) to (1C) of the Act. In the case of a corporate entity, this is defined as:

a) The natural person who ultimately owns or controls the corporate entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings;
b) If, after having exhausted all plausible means,
   i. There is doubt as to whether the person identified under sub-paragraph a) is the beneficial owner; or
   ii. No person under sub-paragraph (a) is identified, the natural person exercising control via other means.
c) If, after having exhausted all possible means,
   i. There is doubt as to whether the person identified under sub-paragraph (b) is the beneficial owner; or
   ii. No person under sub-paragraph (b) is identified, the person is specified under sub-paragraph (d);
d) For the purposes of sub-paragraph (c), the person is:
   i. If the company or legal entity is ultimately owned or controlled through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, by a Listed Entity or a majority owned subsidiary of a Listed Entity, the Listed Entity; and

[14] Section 10(4A), Proceeds of Crime Act 2015

ii. In all other cases, the natural person who holds the position of senior managing official.

35. The Act dictates that the ownership threshold which constitutes a "sufficient percentage of the shares or voting rights" as set out in sub-paragraph (a) above, is 25%. This is regardless of whether the share or ownership interest is held directly in the corporate customer, or indirectly through additional layers of ownership.

36. When identifying and verifying the beneficial owner(s) of any form of corporate entity, the same due diligence requirements apply as in the cases of customers that are natural persons.

5.5.3 Beneficial Ownership of Trusts & Similar Legal Arrangements

37. In the case of trusts, beneficial ownership is defined as[15]:

a) The settlor or settlors;
b) The trustee or trustees;
c) The protector or protectors, if any;
d) The beneficiaries, or where the individuals benefiting from the trust have yet to be determined, the class of persons in whose main interest the trust is set up or operates; and
e) Any other natural person exercising ultimate control over the trust by means of direct or indirect ownership by other means.

38. In the case of other legal entities or arrangements similar to trusts, such as foundations, beneficial ownership refers to the natural person(s) holding equivalent or similar positions to those referred to above, such as[16]:

a) The founder;
b) The foundation councilors;
c) The guardian, if any;
d) The beneficiaries; and
e) Any other natural person exercising control over the foundation or similar legal arrangement.

5.5.4 Publicly Listed Entities

39. In the case of publicly listed entities (as defined under Section 7(1) of the Act), no further steps are required to determine beneficial ownership of the entity. As set out under the Act, the beneficial owner of a publicly listed entity is the entity itself[17]. This concession afforded to listed entities, however, only applies to body corporates with shares admitted to trading on a regulated market[18]:

a) In Gibraltar;
b) In the European Economic Area; or
c) Listed in Schedule 9 of the Act.

40. If an entity is listed on a market which does not fall within the above definition, it cannot be treated as a publicly listed entity for the purposes of applying customer due diligence measures. All beneficial owners must therefore be identified (and where necessary, verified) in accordance with the measures applicable to all other corporate entities.

[15] Section 7(1A)(d), Proceeds of Crime Act 2015
[16] Section 7(1A)(d), Proceeds of Crime Act 2015
[17] Section 7(1A)(b), Proceeds of Crime Act 2015
[18] Section 7(1), Proceeds of Crime Act 2015

41. When dealing with publicly listed entities, a regulated entity should take record of the entity's listing within the public register of the regulated market in question.

5.5.5 Protected Cell Companies ("PCCs")

42. A PCC is a legal vehicle where multiple 'cells' form part of a single legal entity together with a 'core'. A PCC can create an unlimited number of cells, each with segregated assets and liabilities. When conducting due diligence on a PCC, a regulated entity must take into consideration all cells. Likewise, when determining beneficial ownership of a PCC, a regulated entity must consider:

- The ownership structure of each particular cell; and
- The ownership structure of the core.

43. Since a PCC forms a singular collective legal entity, both the core and each cell must be factored into account in understanding the control structure. This is to prevent an individual attempting to conceal their beneficial ownership in the entity by ring-fencing their shares among a spread of different cells. The same requirements apply in relation to establishing beneficial ownership for PCCs as in the case of other corporate entities, as set out under Section 6.4.2.

5.5.6 Limited Liability Partnerships

44. In the case of limited liability partnerships, the identity of all partners should be verified in line with the due diligence requirements applied to individual customers. In cases where the identified partner is not a natural person, steps should be taken to identify and verify beneficial ownership of the entity in line with the relevant requirements outlined above.

45. Where a formal partnership agreement exists, a mandate from the partnership, authorising the opening of an account with the regulated entity in question and conferring authority on those who will operate it, should be obtained.

5.5.7 Clubs, Societies & Management Companies

46. When applying customer identification measures to clubs, societies or management companies, a regulated entity must seek to identify and, on a risk-based approach, verify, the officers of the entity who have authority over any funds or assets. A regulated entity must also take appropriate measures to be reasonably satisfied that the individual(s) in question is appropriately authorised by the club, society or management company.

5.5.8 Charities & Non-Profit Organisations ("NPOs")

47. Charities and NPOs form a crucial part of the global economy, through their efforts in aiding those in need worldwide. It is well known, however, that such organisations are particularly vulnerable to exploitation by criminal actors, including terrorists and terrorist organisations. The risk involving the use of a charity or NPO to disguise the raising and distribution of funds for criminal or terrorist activity is of particular concern where the charity/NPO has connections with high-risk jurisdictions.

48. Most jurisdictions will require charities/NPOs to be publicly registered. The formal registration of a charity/NPO may provide a regulated entity with some level of indication of the legitimacy of the operations. This does not, however, eliminate the risk of the charity/NPO being used as a front for the raising of capital for illicit purposes.

49. In cases where the charity/NPO is a corporate entity, it is likely that there will be no singular individual who will be deemed to hold beneficial ownership as a result of shareholding or

ownership interest. In such cases, in accordance with the Act, the senior managing official would be considered the beneficial owner[19]. This individual must be subject to due diligence measures in line with those set out above for natural persons.

5.5.9 Nominee Shareholdings & Directorships

50. The use of nominee shareholdings and nominee directorships are facilities which introduce complexity to the ownership and control structure of a corporate entity. A regulated entity must have controls in place to identify and assess cases where there has been a misuse of nominee shareholdings or directorships as a means to obfuscate the true beneficial ownership of the entity.

51. The existence of nominee shareholders or directors within the control/ownership structure of a corporate entity will typically increase the level of customer risk posed by that business relationship, and as a result may warrant the application of enhanced due diligence measures. For the purposes of identifying beneficial ownership, a nominee shareholder or director is not considered a beneficial owner of a corporate entity. A regulated entity must identify who the true beneficial owner(s) is by considering:

    a) The person(s) from whom instructions are being taken by the nominee director(s); and/or
    b) The person(s) for whom the shares or interests are being held by the nominee shareholder(s).

5.5.10 Bearer Shares

52. A bearer share, or bearer share warrant, is a physical document that entitles its holder to rights of ownership or title to an underlying property, asset or entity. In such cases, ownership or control is reliant on physical possession of the bearer share document. Beneficial ownership can therefore easily change hands from one individual to another without the awareness or knowledge of the regulated entity.

53. Where a regulated entity's risk appetite includes engaging in regulated activity with a customer whose ownership structure involves the issuance of bearer shares, the regulated entity must have robust controls in place to mitigate the increased risk. The use of bearer shares introduces a significant level of anonymity, which may be misused by those seeking to use corporate entities as vehicles for illicit activity. The existence of bearer shares within the ownership structure of a corporate customer warrants the application of enhanced due diligence measures.

54. In order to mitigate the risk of changes to beneficial ownership occurring without notification to the regulated entity, these bearer shares must be kept immobilised under the control of the regulated entity. In cases where a particular transaction involves bearer instruments, verification evidence must be obtained and recorded for the following transactions:

    a) Bearer shares converting to registered form; and
    b) Surrender of coupons for payment of dividend, bonus or capital event.

55. In order to establish market value, the middle market price quoted from reputable sources on the day of receipt should be documented.

[19] Section 7(1A)(c)(iv)(a), Proceeds of Crime Act 2015

5.6 Exercising Control via Other Means

56. In cases where:

a) There is doubt whether the natural person identified by way of shareholding/ownership as the beneficial owner of a corporate (as set out above) is the true beneficial owner; or

b) No individual has been identified as the beneficial owner;

Beneficial ownership may be attributed to "the natural person exercising control via other means"[20].

57. Identifying such instances in practice is likely to pose a significant level of difficulty and must therefore be considered on a case-by-case basis. Examples of such instances would include:

a) Where a natural person with controlling levels of shareholding/ownership is influenced or dominated by another individual into relinquishing functional control; or

b) Where a natural person is afforded additional legal powers over a corporate entity allowing them to impact decisions taken by those with controlling levels of shareholding/ownership.

5.7 Certification of Documents

58. Where copies of documentation requested as part of a regulated entity's verification measures are provided in the place of true originals, a standard mechanism adopted to mitigate the risk of potential tampering or falsification is to request that the copy is certified by a suitable professional. When assessing the suitability of a potential certifier, a regulated entity should consider a variety of factors, including whether they are:

- In any way connected to or affiliated with the natural person or corporate entity which is seeking certification;
- Based in a jurisdiction with an effective AML/CFT/CPF regime (which does not have a propensity for corruption);
- Of a suitable reputation, and have not been subject to any enforcement/supervisory/legal/civil action or similar; and
- Of a suitable professional background, such as in cases where they are:
    - An accredited member of a professional body; or
    - In a public position subject to high levels of trust.

59. When certification of an identity document is sought by a regulated entity, the regulated entity should ensure that the following information is included within the provided certification:

- The name of the certifier;
- The professional position held by the certifier; and
- A method of contact for the certifier.

60. In the case of business relationships or occasional transactions commenced on a non-face-to-face basis, a regulated entity may request certified identity documents to assure itself that the customer is the true owner of the document. In such cases, a certifier should confirm in writing that the photograph included within the identity document represents a true likeness of the individual in question.

[20] Section 7(1A)(c)(i)(b)

5.8 Reliance

61. Where a business relationship or occasional transaction is introduced to a regulated entity via an introducer, the regulated entity is still required to conduct appropriate due diligence measures in line with the assessed risk profile. The exception to this is in the case of relationships/transactions introduced by an eligible introducer[21].

62. To be an eligible introducer, a third party must meet all four of the following conditions:
    1) It must be regulated by the GFSC (or an equivalent supervisory authority if it carries out business outside of Gibraltar);
    2) It must be subject to equivalent AML/CFT/CPF-related legislative and regulatory requirements;
    3) It must be based in Gibraltar or a country with an equivalent AML/CFT/CPF regime; and
    4) There must be no secrecy or other obstacles which would prevent the Gibraltar regulated entity from obtaining the original without delay when required.

63. Where an introducer satisfies all four of the criteria listed above, a regulated entity may place reliance on the customer identification measures enacted by the eligible introducer, and only request copies of such documentation when necessary. For each business relationship where reliance is placed, the introducer must complete the Eligible Introducer Certificate ("F1 Certificate") available for download on the GFSC website[22]. This certificate must be held by the regulated entity in line with record-keeping requirements.

64. In cases where the regulated entity is required to evidence the application of customer identification measures, the eligible introducer must be able to produce the relevant documentation without delay. When assessing the eligibility of an introducer, a regulated entity must ensure that the introducer complies with AML/CFT/CPF-related requirements which are at least equivalent to those set out locally. In the case of record keeping requirements, for example, the regulated entity must ensure that the introducer will retain records of customer identification documentation in line with the requirements set out under the Act and that the regulated entity may access those at any given time.

5.9 Accounts & Products That Facilitate Anonymity

65. The provision of any form of anonymous accounts, or products that facilitate anonymity, poses a significant level ML, TF & PF risk and are therefore not permitted under the Act or these Guidance Notes. A regulated entity must always seek to identify and verify the identity of its customers, as well as the beneficial owners of those customers.

Sector-Specific Guidance – Virtual Asset Service Providers

66. Virtual Asset Service Providers ("VASPs") (including Distributed Ledger Technology providers) should be aware of the ML/TF/PF risks that certain products and services pose as a result of their ability to obfuscate the identity of the parties involved in a transaction.

67. Privacy-enhancing assets or protocols allow for the concealment of information typically present in a transaction, which facilitates the non-disclosure of user identity. This allows for the obfuscation of the identity of the sender, recipient, holder and/or beneficial owner of the virtual assets in question. For this reason, the GFSC does not permit the use of privacy enhancing

[21] Section 23, Proceeds of Crime Act 2015
[22] Eligible Introducer (F1) Certificate, available under the "Forms" tab.

protocols, or the listing/sale of privacy enhancing assets which have had their privacy-enhancing capabilities enabled.

68. Virtual asset mixing/tumbling services allow for various transactions to be pooled together in order to obfuscate the origin of particular virtual assets, allowing for increased anonymity. These techniques are typically associated with obscuring the identification of "tainted" assets associated with illicit flows or services. For this reason, the GFSC considers the provision of such services to fall outside of its risk appetite and are, therefore, not permitted.

69. For further information on the scope of the VASP registration regime, and those VA activities deemed to fall outside of the risk appetite of the GFSC, please refer to the GFSC's VASP Registration Framework Scope Guidance Note[23]. Further information on the DLT Framework can also be found on the "Distributed Ledger Technology Providers" section of the GFSC website[24].

5.10 Determination of Source of Funds & Wealth

AML/CFT/CPF Requirements

R15 A regulated entity is required to apply a risk-based approach to the establishment and verification of source of funds and wealth of its customers, as well as the beneficial owners behind corporate customers. In the case of customers that do not pose a high level of ML, TF or PF risk, a regulated entity must, as a minimum, assess and document the source of wealth and/or funds to a level that is both plausible and verifiable.

R16 In cases of higher risk, a regulated entity is required to seek independent verification of the source of funds and wealth of its customers, as well as the beneficial owners behind corporate customers.

Guidance

5.10.1 Source of Funds & Wealth

70. In accordance with Section 10(f) of the Act, the application of customer due diligence measures includes "taking a risk-based approach to the verification of source of funds and wealth of a customer and the beneficial owners". Understanding the monetary sources associated with a business relationship is crucial in not only forming an understanding of the level of risk posed by a specific customer but also allows for an assessment of their overall economic profile. It is with this economic profile in mind, that all activity undertaken throughout a business relationship must be scrutinised to aid in the identification of any potentially suspicious activity.

71. In order to undertake a robust assessment a regulated entity must first understand the distinction between source of funds and source of wealth. The FATF defines source of funds as "the origin of the funds or assets which are the subject of the business relationship between the firm and its client and the transactions the firm is required to undertake on the client's behalf (e.g., the amounts being invested, deposited or remitted)". Source of wealth is defined as "the origin of the entire body of wealth (i.e., total assets) of the client".

72. In some cases, the funds and wealth of a customer may be derived from the same source. In cases where a customer has multiple streams of income, their total wealth may have been derived from additional sources. In order to provide a robust economic profile of that customer,

[23] Virtual Asset Service Provider Registration Framework Scope Guidance Note
[24] GFSC Website – Distributed Ledger Technology Providers

they should be asked, on a risk-sensitive basis, to provide information on all forms of income through which they have developed their wealth.

5.10.2 Identification of Source of Funds & Wealth

73. As with other customer due diligence measures, a regulated entity's approach to the identification and verification of source of funds and wealth must be risk-based. The minimum due diligence required on source of funds and wealth to satisfy customer identification documentation on source of funds and wealth is to document this to a level that is both plausible and verifiable. The assessment of source of funds and wealth information in line with this approach has been broken down below.

74. Plausible
Each piece of information provided on a customer's source of funds and wealth should correlate with the regulated entity's collective assessment of the economic profile of that customer.

75. Verifiable
The information provided on a customer's source of funds and wealth should be to a level of detail that would enable the regulated entity, law enforcement agencies or other relevant bodies, to verify the information if the customer's risk profile increases; or if ML, TF or PF was known or suspected.

Example – Plausibility & Verifiability of Source of Funds & Wealth Information

76. When asked to provide information on source of funds and wealth, a prospective low risk customer responds with the following: "*salaried employee, earning over 250k*".

77. Based on the information provided, a regulated entity would be unable to determine the plausibility of this individual's economic profile. This is because no information has been provided on the individual's place of work, the sector that they operate in, or the role that they hold. A regulated entity would be unable to determine whether a salary of that amount, for example, would be plausible in that given scenario. If the risk profile of that customer were to increase or their pattern of transactions were to change, the regulated entity may also have difficulty in verifying whether this activity is still in line with the customer's economic profile. In the example provided above, this is in part due to the annual salary amount of the individual being defined as anything "over 250k" and not a specific figure, which is very wide-ranging.

5.10.3 Independent Verification of Source of Funds & Wealth

Guidance

78. In cases of higher risk, it is not considered adequate to apply standard due diligence measures. A regulated entity must instead apply enhanced due diligence measures. In such cases, a regulated entity is required to seek independent verification of source of funds and wealth of their customers, as well as the beneficial owner(s) of those customers. In addition to instances where a regulated entity has risk profiled a customer as high risk, independent verification must also be sought for PEPs, as well as family members and close associates of PEPs.

79. Independent verification requires that a regulated entity corroborate the information provided by its customer using reliable and independent sources. The type of document or source of information that would satisfy this requirement, is likely to depend on the nature of the customer's income or wealth. A non-exhaustive list of corroborating examples for source of funds and wealth information has been included below:

Table 1 – Corroborating Examples of Source of Wealth/Funds Documentation

Source of Wealth/Funds	Examples of Corroborating Information
Company Sale	- Copy of the contract of sale; - Internet research of Company Registry; - Name and address of Company; - Total sales price; - Applicants' share participation; - Nature of business; - Date of sale and receipt of funds; - Media coverage.
Company Profits/Dividends	- Copy of latest audited financial statements; - Copy of latest management accounts; - Board of Directors approval minutes; - Dividend distribution; - Tax declaration form.
Inheritance	- Name of deceased; - Date of death; - Relationship to applicant; - Date received; - Total amount; - Solicitor's details; - Tax clearance documents.
Employment Income	- Nature of employer's business; - Name and address of the employer; - Annual salary and bonuses for the last couple of years; - Last month/recent pay slip; - Confirmation from the employer of annual salary; - Latest accounts or tax declaration if self employed.
Savings/Deposits	- Bank statement and enquiry on source of wealth.
Property Sale	- Details of the property sold; - Copy of contract of sale; - Title deed from land registry
Sale of shares or other investment	- Copy of contract; - Sale value of shares sold and how they were sold; - Statement of account from agent; - Transaction receipt/confirmation; - Shareholder's certificate; - Date of sale.
Loan	- Loan agreement; - Amount, date and purpose of loan; - Name and address of lender; - Details of any security.
Gift	- Date received; - Total amount; - Relationship to applicant; - Letter from donor explaining reason for the gift; - Certified identification documents of donor; - Source of wealth documentation of donor
Maturity/surrender of life policy	- Amount received;

	- Policy provider; - Policy number/reference; - Date of surrender.
Other income sources	- Nature of income (amount, date received, who from); - Appropriate supporting documentation.

80. In the case of high net worth individuals, it may be difficult to assess the entirety of their income or wealth as a result of its complexity. In these cases, the extent of verification required should be in line with the risk profile of the individual and if considered higher risk, include independent verification of at least the majority of the customer's income or wealth.

81. Where open source information is available on the source of funds or wealth of a customer, this can also be used for verification purposes. This is only considered appropriate, however, in cases where the information comes from a source that is both reputable and independent (i.e. not derived directly from the customer, the customer's website or any individual/entity associated with the customer).

5.10.4 Establishing Source of Wealth & Funds of Corporate Customers

82. In the case of a corporate customer, the requirement to identify and verify source of funds and wealth extends to its beneficial owners, regardless of whether or not the corporate entity's funds are derived from those individuals. This is because of the risk that the beneficial owners are in a position to potentially transmit illicit funds through the legitimate business operations of the corporate customer. In cases where a beneficial owner has not transmitted their own funds into or through the corporate customer in question, the requirement would solely apply to identify and verify their source of wealth.

5.11 Acquisitions of Business

83. When a regulated entity acquires the business of another financial services provider (either in whole or as part of a portfolio or "book"), it is not necessary for the identity of all existing customers to be re-established, provided that:

a) All records relating to those customers are acquired with the business; and
b) The financial services provider in question has applied AML/CFT/CPF measures equivalent to those applicable within Gibraltar.

84. Prior to engaging in the acquisition of business from another financial services provider, a regulated entity must conduct the necessary due diligence to ensure that it is not exposing itself to undue levels of risk. In cases where a regulated entity has determined that its acquisition does not satisfy the requirements listed above, adequate customer identification measures must be established prior to the on-boarding of any of the acquired business.

85. A regulated entity must also consider whether each individual business relationship forming part of the proposed book/portfolio of business, falls within its risk appetite.

5.12 Simplified Due Diligence Measures

5.12.1 Application of Simplified Due Diligence ("SDD") Measures

86. Simplified due diligence is the minimal level of due diligence that can be applied to a business relationship or occasional transaction. Under the Act, this is only permissible where there is a low risk of ML, TF, and PF. A regulated entity may apply SDD measures in cases where, following

a risk assessment, the entity has established that the business relationship or transaction presents a lower degree of risk of ML, TF and PF risks and there are no suspicions or knowledge of ML, TF, or PF[25].

87. SDD allows a regulated entity to adjust the extent of the verification applied as part of its due diligence measures in a way that is proportionate to the lower risk that has been identified. It is not an exemption from applying the customer due diligence measures under POCA. The regulated entity must carry out its customer risk assessment including the four risk areas before it can conclude that SDD measures can be applied. These risk factors must include customer, product, country and interface risk factors. This will indicate whether there is, in fact, a low risk of ML, TF or PF. Further guidance on customer risk assessments can be found within the "Customer Risk Assessment" section of these Guidance Notes. A regulated entity must be able to demonstrate that it has taken all necessary steps and have reasonable grounds for deeming that the customer or transaction falls within one of the categories set out in Schedule 6 of the Act.

88. It is important to note that there is no mandatory requirement to apply SDD measures. A regulated entity may therefore elect to apply standard customer due diligence measures in instances of low identified risk where SDD is not deemed appropriate. Instead, Schedule 6 of the Act includes a non-exhaustive list of risk factors which may be used as a guide to determine factors which pose a lower risk by the business relationship/occasional transaction. There are a range of factors to consider when assessing whether there is a low risk of ML, TF or PF and this will typically be dependent on the type of relationship which is being established.

Schedule 6 of the Act provides a non-exhaustive list of factors and types of potentially lower risk relationships that could justify the application of simplified due diligence.[26]These risk factors have been set out within each of the sections included below.

5.12.2 Customer Risk Factors

89. The following factors are examples of instances that would lead to a decreased perceived level of customer risk:

- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- Public administrations or enterprises;
- Customers that are resident in geographical areas of lower risk.

5.12.3 Product, Service, Transaction or Delivery Channel Risk Factors

90. The following factors are examples of instances that would lead to a decreased level of product, service, transaction or delivery channel risk:

- Life insurance policies for which the premium is low;
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;

[25] Section 16(1), Proceeds of Crime Act 2015
[26] Schedule 6, Proceeds of Crime Act 2015

- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
- Products where the risks of ML and TF are managed by other factors such as purse limits or transparency of ownership (e.g., certain types of electronic money).

5.12.4 Geographical Risk Factors

91. Residence, establishment or registration in the following jurisdiction would be considered to pose a decreased level of geographic risk:
    - Gibraltar;
    - Third countries having effective AML/CFT/CPF systems;
    - Third countries identified by credible sources as having a lower level of corruption or other criminal activity;
    - Third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat ML, TF and PF consistent with the revised FATF Recommendations and effectively implement those requirements.

92. Where a regulated entity has concluded it may apply SDD measures, it must continue to comply with the customer due diligence requirements under Section 10 of the Act. Regardless of the determination of a lower level of ML/TF/PF risk and application of SDD measures, a regulated entity must continue to conduct adequate ongoing monitoring of those business relationships and transactions in keeping with the provisions under Section 12 of the Act[27]. This requirement is crucial as it allows a regulated entity to identify any unusual or suspicious activity or transactions.

5.12.5 Natural Persons

93. If a regulated entity determines that it is appropriate to conduct SDD measures on a natural person, it would be expected to collect, as a minimum,:
    - The name of the individual;
    - The residential address of the individual;
    - The contact details of the individual; and
    - Information on the source of funds and wealth of the individual to a level of plausible verifiability.

5.12.6 Legal Entities, Legal Arrangements or similar (collectively known as "Legal Entities" or "Corporate Entities")

94. If a regulated entity determines that it is appropriate to conduct SDD measures on a legal entity, it would be expected to document, as a minimum:
    - The name of the entity, including any trading or business names;
    - The number of incorporation/registration, or equivalent;
    - The legal form of the entity;
    - The date of incorporation/registration;
    - The country or countries of registration and activity;
    - The registered office address;
    - Information relating to each of the beneficial owners, as specified under Section 6.10.2 of these Guidance Notes; and

[27] Section 16(2), Proceeds of Crime Act 2015

- Information on the source of funds and wealth of both the entity and the beneficial owners to a level of plausible verifiability.

95. The examples set out below provide cases where SDD may or may not be applied in respect of customers that are corporate or legal entities. Please note that these examples are illustrative only and any similar case should be subject to the outcome of the regulated entity's risk assessment which must be considered as a whole.

Example – Well-Established Public Company in a Low-Risk Industry

Scenario

A regulated entity is considering providing banking services to a well-established public company that is listed on a regulated market within the EEA. The company operates in a low-risk industry with a long history of transparent financial reporting and compliance.

Why would simplified due diligence be appropriate in the above scenario?

96. Public companies listed on regulated markets are typically required to comply with strict financial reporting standards and regulations. They may be subject to regular audits, and their financial statements may be publicly available. This transparency provides a level of assurance regarding the company's financial health and reduces the need for extensive due diligence on financial information.

97. Public companies are typically subject to significant regulatory oversight and inspection by regulatory bodies. These regulatory bodies monitor the company's compliance with disclosure requirements, corporate governance requirements, and other regulatory obligations. The existence of such oversight contributes to a lower risk profile and supports the application of simplified due diligence.

98. Publicly listed companies are typically required to disclose relevant information to the market. This information includes financial reports, annual reports, press releases, and disclosures of material events. Financial firms can access and analyse this publicly available information to gain insights into the company's operations, performance, and corporate governance practices, thereby facilitating simplified due diligence.

99. When determining the level of due diligence that should be applied to a publicly listed entity, a regulated entity must take into account the reputability of the market within which the entity has been listed. While concessions are afforded under Section 7(1A)(b) of the Act in determining the beneficial ownership of a listed entity, this only applies to entities listed on a regulated market in Gibraltar, the EEA, or otherwise listed within Schedule 9 of the Act[28].

[28] Section 7(1), Proceeds of Crime Act 2015

Example – High-Risk Jurisdiction and Complex Ownership Structure

Scenario

A regulated entity is considering establishing a business relationship with a potential customer who operates in a high-risk jurisdiction which is known for its weak regulatory regime and prevalent financial crime. The potential customer is a company with a complex ownership structure involving multiple layers of ownership and offshore entities.

Why would simplified due diligence not be appropriate in the above scenario?

100. In high-risk jurisdictions that have a lack of regulatory oversight, financial services firms face a higher likelihood of encountering customers involved in money laundering, terrorist financing and/or proliferation financing. Simplified due diligence typically involves reducing the extent of assessment and verification, which can undermine compliance with regulatory duties and increase the risk of inadvertently engaging with individuals/companies who are engaging in illicit activities.

101. The complexity of the ownership structure and the involvement of offshore entities raise red flags for potential illicit activities, such as hiding the identities of beneficial owners. Simplified due diligence may not sufficiently capture the details of the structure and the associated risks. Thorough due diligence, including enhanced measures, is necessary to assess the legitimacy and reliability of the potential customer.

102. Operating in a high-risk jurisdiction and establishing relationships without thorough due diligence can expose a regulated entity to significant reputational risks. If a potential customer is involved in illegal activities, it can damage the firm's reputation and break down customer trust. A regulated entity must, therefore, demonstrate a commitment to apply robust due diligence measures to mitigate such risks.

103. Applying simplified due diligence in a situation that requires more comprehensive scrutiny may lead to regulatory non-compliance and thus, potential supervisory penalties or consequences for the regulated entity.

5.13 Enhanced Due Diligence ("EDD") Measures

AML/CFT/CPF Requirements

R17 A regulated entity must apply enhanced due diligence measures in scenarios which it deems to pose a higher level of ML, TF and PF risk, such as those set out within these Guidance Notes and Schedule 7 of the Act[29]. The measures applied should be commensurate with the risks posed by the business relationship/occasional transaction, taking into account product, interface, customer and country risk factors.

[29] Schedule 7, Proceeds of Crime Act 2015

R18 A regulated entity must apply enhanced due diligence measures to customers established in high-risk jurisdictions[30].

Guidance

104. Conducting enhanced due diligence involves applying additional verification measures to independently corroborate the information provided by a prospective customer. EDD is a vital tool when dealing with business relationships or occasional transactions that present a higher level of ML/TF/PF risk. This guidance aims to outline the potential higher risk factors that a regulated entity should consider when determining the application of EDD measures.

105. Schedule 7 of the Act provides a non-exhaustive list of factors and types of potentially higher risk relationships that impose the application of enhanced due diligence. These risk factors have been set out within each of the sections included below.

5.13.1 Customer Risk

106. The following factors are examples of instances that would lead to an increased perceived level of customer risk:

- Business relationships occuring under unusual circumstances;
- Customers residing in high-risk geographical areas;
- Legal entities or arrangements functioning as personal asset-holding vehicles;
- Companies with nominee shareholders or shares held in bearer form;
- Cash-intensive businesses;
- The ownership structure appears excessively complex or unusual considering the nature of business; and
- Customers who are third-country nationals seeking residence rights or citizenship in exchange for capital transfers, property purchase, government bonds, or investments in corporate entities within that country.

5.13.2 Product, Service, Transaction & Delivery Channel Risk

107. The following factors are examples of instances that would lead to an increased level of product, service, transaction or delivery channel risk:

- Private banking services;
- Products or transactions that enable anonymity;
- Companies under management which pose a level of increased risk;
- Cash intensive businesses;
- Non-face-to-face business relationships or transactions without adequate safeguards, such as electronic signatures, identification means, or trusted electronic identification processes recognised or approved by the relevant supervisory body;
- Receipt of payments from unknown or unaffiliated third parties;
- Introduction of new products, business practices, delivery mechanisms, and emerging technologies for both new and existing products; and
- Transactions involving oil, arms, precious metals, tobacco products, cultural artifacts, archaeological/historical/cultural/religious items, rare scientific valuables, ivory, protected species, or other potentially high risk markets.

5.13.3 Geographical Risk

108. The following factors are examples of instances that would lead to an increased level of geographical risk:

[30] Section 17(1)(b), Proceeds of Crime Act 2015

- Countries lacking effective (AML/CFT/CPF) systems, as identified by credible sources such as those involving mutual evaluations, detailed assessment reports, or published follow-up reports;
- Countries identified by credible sources as having significant levels of corruption or other criminal activities;
- Countries subject to sanctions, embargoes, or similar economic measures; and
- Countries identified as providing funding or support for terrorist activities or hosting designated terrorist organizations.

5.13.4 Additional Risk Factors

109. In addition to the factors outlined in the Act, the GFSC has specified additional risk factors that should be taken into account to identify higher-risk situations. This non-exhaustive list of factors have been set out in Sections 16.13.5 to 16.13.8 and should be taken into consideration when risk assessing both prospective and new customers.

5.13.5 Politically Exposed Persons (PEPs)

110. A regulated entity must apply enhanced due diligence measures for PEPs, their family members, and close associates as defined in Section 20A of the Act. This applies regardless of the geographical location of the PEP or other potential lower risk factors.

5.13.6 National Risk Assessment

111. A regulated entity should be sufficiently familiar with the HM Government of Gibraltar National Risk Assessment to understand the threats and vulnerabilities associated with specific products or services present in the jurisdiction and/or specific sector. The NRA may also list countries and territories that are considered to pose a higher risk to Gibraltar. A regulated entity must ensure that any information published in the NRA is incorporated into the entity's risk methodology and scoring mechanism.

5.13.7 Ministerial Notices & Information

112. If a risk is classified as high through a notice published in the Gazette, or if the National Coordinator for Anti-Money Laundering and Combatting Terrorist Financing Regulations 2016 states any factors which indicate a high-risk product, service, country or customer, enhanced due diligence measures must be applied.

5.13.8 High-Risk Business Relationships

113. If a regulated entity identifies a business relationship as high risk based on its own risk methodology, enhanced due diligence measures must be applied, unless the entity can provide a documented justification for otherwise and apply mitigating factors accordingly.

5.13.9 Branches and Majority-Owned Subsidiaries in High-Risk Third Countries

114. In the event that a Gibraltar-based regulated entity has a branch or majority-owned subsidiary located in a high-risk third country, enhanced due diligence measures are not required if the group adheres to Gibraltar's AML/CFT/CPF requirements and these Guidance Notes. The regulated entity must demonstrate appropriate oversight over the branch’s/subsidiary's application of Gibraltar's AML/CFT/CPF measures.[31]

5.13.10 Outsourced Providers in High-Risk Jurisdictions

[31] Reliance – Section 23(1B), Proceeds of Crime Act 2015

115. Enhanced due diligence measures are not required to be carried out by a regulated entity on an outsourced provider based in a high-risk jurisdiction if the provider is compliant with Gibraltar legislative and regulatory requirements. Nonetheless, a regulated entity may wish to take this into consideration as best practice.

5.13.11 Application of Enhanced Due Diligence Measures

116. When applying enhanced due diligence measures the regulated entity should take the following steps to verify the information provided by the applicant for business.

117. Business Relationship:
A regulated entity is required to gather comprehensive information about the nature and purpose of the business relationship with the customer. This includes understanding the scope of the services or transactions involved, the expected duration of the relationship and its intended nature and purpose. The process may also involve assessing the customer's industry, business activities, and the potential risks associated with the proposed relationship.

118. Purpose & Scope of the Business Relationship:
A regulated entity must understand the underlying reasons for establishing a particular business relationship. By understanding the purpose, the regulated entity can assess the legitimacy of the relationship and ensure that it falls within its own risk appetite. This will also involve determining the type and volume of anticipated transactions, the frequency of interactions and any arrangements or services requested.

119. Obtaining information about the specific activities the customer intends to carry out within the business relationship is key. This can include details such as anticipated financial flows, intended counterparties, geographic locations involved and any other relevant factors. By understanding the expected activities, a regulated entity can assess the potential exposure to ML/TF/PF.

120. In some cases, a regulated entity may request supporting documentation to substantiate the intended nature of the business relationship. This can include business plans, contracts, project details, or any other relevant documents that provide additional insight into the customer's objectives and activities. By gathering additional details on the intended nature of the business relationship, a regulated entity can better assess the associated risks, tailor its due diligence measures accordingly, and ensure that the relationship aligns with regulatory requirements and its own risk management framework.

121. Beneficial Owners:
A regulated entity is required to collect enhanced documentation on the beneficial owners involved. This information helps verify who holds the ultimate decision-making power and financial interests within legal entities.

122. Independent Verification of Source of Wealth & Funds
Seeking independent verification of the source of funds and source of wealth of the customer and the beneficial owner(s) involves obtaining objective and reliable information from external, independent sources to confirm the legitimacy and origin of the funds and wealth involved in the business relationship.

123. A key part of the establishment of enhanced measures is the verification of source of wealth and funds applied during the business relationship. When applying enhanced measures, getting the applicant for business documenting the source of funds and wealth will not be sufficient. A regulated entity must seek to independently verify the origin of these funds. Section 6.10.3

highlights examples of the type of documentation a regulated entity can request from the applicant for business for verification purposes.

124. A regulated entity may use independent data sources to verify the nature of the source of wealth and funds of the beneficial owner(s). These independent sources ensure that the information obtained has not been subject to manipulation by the applicant for business or customer.

125. Rationale for the Intended or Completed Transactions
Requesting information regarding the rationale for the intended or completed transactions involves seeking clarification from the customer about the purpose and reasoning behind the specific financial transaction or activity in line with the business relationship.

126. A regulated entity needs to gain insight into the purpose and rationale behind the transactions to assess the legitimacy and potential risks. This may involve asking the customer to provide a clear explanation of why is engaging in a particular transaction or series of transactions. Understanding the rationale helps determine if the activities align with the customer's usual or anticipated business, expected turnover and whether is in keeping with what the customer outlined when establishing the business relationship.

127. Requesting further information also helps identify any red flags or suspicious elements associated with the transactions. If the explanation provided by the customer appears vague, inconsistent, or does not align with the established business activities, it may indicate that illicit activity is taking place. In such cases, further scrutiny and enhanced due diligence measures may be necessary.

128. Documenting the purpose of the business
A regulated entity should maintain proper documentation of the rationale provided by the customer. This documentation serves as evidence that the business relationship and associated transactions are in line with expectations and that the regulated entity has taken appropriate steps to verify this.

5.13.12 Senior Management Approval

129. Before establishing a new high risk business relationship or occasional transaction (or when determining to continue an existing one at the point of periodic review or upon a trigger event), a regulated entity should consider obtaining senior management review and approval. This should be documented alongside any risk mitigation strategy devised by the senior management team. The following are instances where obtaining senior management approval is deemed mandatory under the Act:

- When establishing or continuing a business relationship or occasional transaction involving a high risk jurisdiction[32]; and
- When establishing or continuing a business relationship with a Politically Exposed Person (including a close associate or family member of a Politically Exposed Person)[33].

5.13.13 Enhanced ongoing monitoring of the business relationship

130. Enhanced ongoing monitoring refers to an increased level of scrutiny that a regulated entity must implement for high-risk business relationships. It will involve continuously monitoring and assessing the activities, transactions, and behaviours of these relationships to detect and

[32] Section 16(6)(e), Proceeds of Crime Act 2015
[33] Section 20(1)(a), Proceeds of Crime Act 2015

mitigate any potential risks associated with ML, TF or PF. Ongoing monitoring, including enhanced ongoing monitoring requirements, is covered within the "Ongoing Monitoring" section of these Guidance Notes.

5.14 Wire Transfers

Sector-Specific Guidance – Payment Services

131. Investigations into major money laundering cases in recent years have shown that criminals make extensive use of electronic payment and messaging systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity associated with such cases and the ability to trace each transaction.

132. Requirements relating to wire transfers apply to the transfer of funds, in any currency, which are sent or received by a Payment Service Provider ("PSP") established in Gibraltar[34]. The requirements do not apply to transfers of funds:

a) Carried out using a payment card, an electronic money instrument or a mobile phone, or any other digital or IT repaid or postpaid device with similar characteristics (unless used in order to effect a person-to person transfer of funds), where:
   i. The card, instrument or device is used to pay for goods or services; or
   ii. The unique identifying number of that card, instrument or device accompanies all transfers flowing from the transaction.
b) Where the payer withdraws cash from their own payment account;
c) Where the funds are issued to a public authority as payment for taxes, fines or other levies;
d) Where both the payer and payee are payment service providers acting on their own behalf;
e) That are carried out through cheque image transfers, including truncated cheques;
f) Where the service provided does not constitute a payment service, as listed within points (a) to (m) and (o) of Schedule 2, Part 4, Paragraph 18 of the Financial Services Act 2019[35]; or
g) Carried out within Gibraltar to a payee's payment account permitting payment exclusively for the provision of goods or services where:
   i. The payment service provider of the payee is subject to the Proceeds of Crime Act 2015;
   ii. The payment service provider of the payee is able to trace back, through the payee, by means of a unique transaction identifying, the transfer of funds from the natural or legal person who has an agreement with the payee for the provision of goods or services; and
   iii. The amount of the transfer does not exceed EUR 1,000.

133. Where both the PSP of the payer and payee are situated within Gibraltar, the United Kingdom or the EU, transfers of funds are required to be accompanied by at least the account number of both the payer and payee, or a unique identifier as long as it allows the transaction to be traced back to the payer. If requested by the PSP of the payee, however, complete information on the payer should be issued within three working days of that request.

[34] Regulation (EU) 2015/847 of the European Parliament and of the Council
[35] Schedule 2, Part 4, Paragraph 18, Financial Services Act 2019

134. For domestic wire transfers (i.e. within Gibraltar), PSPs should ensure that the information accompanying the transfer is the same as is required for cross-border wire transfers.

135. Where a transfer of funds is made to a payee's PSP situated outside of the UK or EU, this must be accompanied by the following information on the payer:

- The full name of the payer;
- The address of the payer (alternatively substituted by the individual's date of birth, customer identification number or national identity number); and
- The account number of the payer (or equivalent unique identifier).

136. In the case of such transfers, the PSP of the payer must verify the information on the payer only where the amount exceeds EUR 1,000, unless the transaction is carried out in several operations that appear to be linked and together exceed EUR 1,000.

137. Intermediary PSPs must ensure that all originator and beneficiary information that accompanies a wire transfer is retained within it. They should also take reasonable measures to identify cross-border wire transfers that do not contain all required originator and/or beneficiary information.

138. Payment service providers must ensure that all originator and beneficiary information is retained in keeping with the record keeping requirements set out under the Act.

139. In the case of batch file transfers, the individual transfers bundled together need not include the information listed within paragraph 143, provided that the batch file contains that information and that the individual transfers carry the account number of the payer or a unique identifier.

140. The PSP of the payee should take reasonable measures (either in the form of post-event monitoring, or real-time monitoring where available), to identify cross-border wire transfers that lack required originator information or required beneficiary information. If the payment service provider of the payee becomes aware, when receiving transfers of funds, that information on the payer required is missing or incomplete, it must either reject the transfer or ask for complete information on the payer. The PSP should also consider whether a report to GFIU should be made. In the case of the repeated failure to supply the required information, the PSP should consider escalating matters appropriately.

5.15 The Travel Rule

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

141. As in the case of wire transfers, VASPs are also required to transmit and receive information when acting as the originator or beneficiary of a virtual asset transaction which is equal to or exceeding EUR 1,000[36]. In the case of an originator VASP sending a virtual asset transfer to another VASP (irrespective of whether the transfer is made on its own account), the entity in question must receive the following information[37]:

a) The payee's name;
b) The payee's virtual asset account number;
c) The payer's name;
d) The payer's virtual asset account number;
e) Where the payee or the payer does not have a virtual asset account number, a unique transaction identifier; and
f) One of the following:

[36] Proceeds of Crime Act 2015 (Transfer of Virtual Assets) Regulations 2021
[37] Regulation 4, Proceeds of Crime Act 2015 (Transfer of Virtual Assets) Regulations 2021

i. The payer's address;
ii. The payer's national identity number;
iii. The payer's customer identification number; or
iv. The payer's date and place of birth.

142. Where a beneficiary VASP receives a virtual asset transfer equal to or above the EUR 1,000 threshold from another VASP, the beneficiary VASP must ensure that it receives the information specified above, as well as corroborates the consistency of that information with its own records[38].

143. In cases where the beneficiary VASP receives a virtual asset transfer equal to or above the EUR 1,000 threshold from a person that it not a VASP, the beneficiary entity must ensure that it obtains the following information[39]:

a) The payer's name;
b) The payer's address;
c) The payer's national identity number;
d) The payer's customer identification number; and
e) The payer's date and place of birth.

144. VASPs must ensure that the transfer of information is made on an immediate and secure basis, and that all information is held in line with the record keeping requirements set out under Section 25 of the Proceeds of Crime Act 2015[40]. It is the responsibility of the VASP to identify an appropriate solution to facilitate the transmission of such information.

[38] Regulation 5(1), Proceeds of Crime Act 2015 (Transfer of Virtual Assets) Regulations 2021
[39] Regulation 5(2), Proceeds of Crime Act 2015 (Transfer of Virtual Assets) Regulations 2021
[40] Regulation 6(2), Proceeds of Crime Act 2015 (Transfer of Virtual Assets) Regulations 2021

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