PRIVATE SECTOR CONSULTATION

Amendments to Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (5 June 2020)– e-KYC and Remote CDD/Ongoing Monitoring

Private Sector Consultation
Amendments to Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (5 June 2020) – e-KYC and Remote CDD/Ongoing Monitoring

A. Introduction

1. Section 34(1)(a) of the Monetary Authority Act (2020 Revision) ("MAA") states that:

After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may –

a) issue or amend rules or statements of principle or guidance concerning the conduct of licensees and their officers and employees, and any other persons to whom and to the extent that the regulatory laws may apply;
b) issue or amend statements of guidance concerning the requirements of the anti-money laundering regulations or the provisions of the regulatory laws; and
c) issue or amend rules or statements of principle or guidance to reduce the risk of financial services business being used for money laundering or other criminal purposes.

2. Requirements specific to the private sector consultation are outlined in section 4(1) of the MAA as follows:

When this Law requires private sector consultation in relation to a proposed measure –

a) the Authority shall give to each private sector association a draft of the proposed measure, together with –

i. an explanation of the purpose of the proposed measure;
ii. an explanation of the Authority's reasons for believing that the proposed measure is compatible with the Authority's functions and duties under section 6;
iii. an explanation of the extent to which a corresponding measure has been adopted in a country or territory outside the Islands;
iv. an estimate of any significant costs of the proposed measure, together with an analysis of the benefits that will arise if the proposed measure is adopted; and
v. notice that representations about the proposed measure may be made to the Authority within a period specified in the notice (not being less than thirty days or such shorter period as may be permitted by subsection (3)); and

b) before proceeding with the proposed measure, the Authority shall have regard to any representations made by the private sector associations, and shall give a written response, which shall be copied to all the private sector associations.

3. The Cayman Islands Monetary Authority ("the Authority") seeks consultation and comment from the private sector associations concerning the proposed:

a) Amendments to Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (5 June 2020) – e-KYC and Remote CDD/Ongoing Monitoring ("Guidance Notes") (**Appendix 1)**.

B. Background

4. Regulations 12(1)(a) of the Anti-Money Laundering Regulations, 2020 ("AMLRs") and section 4A3(1) of the Guidance Notes require the verification of a customer's identity to be done using "reliable, independent, source documents, data or information", and does not prescribe the manner in which this should be done.

5. However, during the COVID-19 pandemic in 2020, the Authority issued an advisory[1] which provided for alternative ways to verify information (both at the time of establishing relationships and/or as part of ongoing customer due diligence) whilst observing curfew, social distancing or self-isolation. The Advisory also included the statement "Where a regulated entity has adopted a deviated verification method, it should complete the verification using normal processes as soon as practicable". There was no definition of what constituted "normal processes", just that it referred to measures which were outside of the regulated entity's standard procedures. This suggested that remote/virtual/non-face-to-face onboarding and ongoing CDD was not standard practice, firstly through the advisory "allowing" regulated entities to use such procedures in light of COVID-19, and subsequently the directive to revert to "normal processes".

6. The 2020 advisory published by the Authority suggested that regulated entities could use virtual means of verification to address the needs of covid-related social distancing but should "complete the verification using normal processes as soon as practicable". This placed a potentially onerous task on the industry to go back and obtain documentation for all clients onboarded during lockdown.

C. International Standards

7. The proposed amendments to the Guidance Notes support the FATF-issued guidance on digital identification[2] ("ID") which was published in March 2020. The key points are as follows:

a) Countries should consider revising policies that automatically classify non-face-to-face business as high risk to the extent that digital ID may be used reliably to identify and verify the identities of customers.

b) FSPs may consider assigning a standard or low-level risk rating when utilising digital ID systems or e-KYC technology with appropriate assurance levels or have been tested and approved by government or an approved expert body.

c) FSPs must ensure that the level of assurance is adequate to the jurisdiction, product, customer and assessed ML/TF risks of the scenarios to which the system is being applied.

d) FSPs should understand the basic components of digital ID systems and technological solutions and take an informed risk-based approach to relying on these for remote onboarding/ongoing monitoring.

e) FSPs should carry out formal risk assessments of new e-KYC/digital ID technology which include documented consideration of how the proposed system works, the level of assurance it provides, and any risks associated with it.

[1] 'Anti-Money Laundering and Countering the Financing of Terrorism compliance during COVID-19'
[2] March 2020 – FATF, Digital Identity

D. Purpose of Proposed Measures and Consistency with the Authority's Functions

8. Section 6(1) of the MAA provides that the principal regulatory functions of the Authority include, to:

"(b)(ii) to monitor compliance with the anti-money laundering regulations; …"

9. Section 6(3) of the MAA further provides that in performing its regulatory functions the Authority, shall:

"(b) endeavour to reduce the possibility of financial services business or relevant financial business being used for the purpose of money laundering or other crime;…"

10. Regulation 12(1)(a) of the AMLrs prescribes that a person carrying out relevant financial business, shall:

"(a) identify a customer, whether a customer in an established business relationship or a one-off transaction, and whether natural, legal person or legal arrangement and shall verify the customer's identity using reliable, independent source documents, data or information;…"

11. The purpose of the proposed guidance notes is to remove any ambiguity on whether the use of technological solutions for remote/virtual/non-face-to-face CDD is permitted beyond the context of COVID-19 and clarify that Financial service providers ("FSPs") need only conduct further verification on a risk-based approach, on a case-by-case basis, dependent on the risk factors and scenarios presented.

E. Proposed Amendments to the Guidance Notes

12. The following is a table of amendments being proposed to the Guidance Notes (refer to **Appendix 1** for the amended Guidance Notes). Amendments to sections can be seen in blue font for ease of reference in Table 1 below:

Table 1: Proposed Amendments to the Guidance Notes (amendments presented in blue font)

Reference:	**Proposed Amendment/New Provision**
Section 3 B (7) ***Assessing Risk and RBA*** ***Inclusion of RBA for Digital ID/ technological***	1. As a part of the RBA, FSPs should: (1) identify ML/TF risks relevant to them; (2) assess ML/TF risks in relation to: (a) their applicants/customers (including beneficial owners); (b) Country or geographic area in which persons under (a) above reside or operate and where the FSP operates; (c) products, services and transactions that the FSP offers; and (d) their delivery channels[3], including remote onboarding[4] and ongoing monitoring of business relationships. **Inclusion of the definition for remote onboarding in the footnote:**

[3] Delivery channel in this context is the way/means whereby an FSP carries its business relationship and/or occasional transaction with a customer, e.g. directly or through other means such as email, internet, intermediary, or any correspondent institution.
[4] Remote onboarding is the establishment of new business relationships via technology and non-face-to-face means where the customer is not physically present at the place where the relationship is being established.

Reference:	**Proposed Amendment/New Provision**
	• Remote onboarding is the establishment of new business relationships via technology and non-face-to-face means where the customer is not physically present at the place where the relationship is being established.
Section 3 C (New provisions 7&8) ***Identification and Assessment of Risk***	7. Customer identification and verification methods should align with the FSP's risk assessment of the client so the decision to onboard a customer remotely, using e-KYC methods and digital ID technologies is required on a case-by-case basis, dependent on the risks presented and assessed. 8. Where the customer, product, service, or jurisdiction is identified as higher risk for ML/TF, the FSP should conduct additional verification measures to ensure the accuracy of e-KYC procedures. The FSP may also consider not using e-KYC or remote onboarding for the establishment of the business relationship or for performing ongoing CDD but reverting to face-to-face interactions or reviewing original certified documents, for example.
Section 3 D ***Product, Services and Delivery Channels Risk Factors*** ***(New Section and provisions 13- 16)***	Risk Assessment of Technology Solutions 13. FSPs should consider the basic components of digital ID/e-KYC[5] systems and take an informed risk-based approach to relying on these when conducting non-face to face onboarding or ongoing monitoring of business relationships. This includes understanding a chosen system's assurance levels and ensuring that those levels are appropriate to the assessed money laundering/terrorist financing risks of the scenarios/cases to which the system is being used. FSPs must ensure the level of assurance is adequate for the jurisdiction, product, customer etc. 14. FSPs should carry out formal risk assessments of new e-KYC/digital ID technology which include documented consideration of how the proposed system works, the level of assurance that it provides, and any particular risks associated with it. 15. The use of video-conferencing[6], as with other forms of non-face-to-face measures must be in accordance with a risk-based approach. FSPs should put in place appropriate controls during the video-conferencing

[5] A digital ID system is a system that covers the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital.- FATF Guidance on Digital ID, 2020
E-KYC refers to the processes whereby a customer's identity is verified via electronic means.

[6] Video-conferencing is a live, visual and audio method of communication connection between two or more remote parties over the internet that stimulates a face-to-face meeting.

Reference:	**Proposed Amendment/New Provision**
	process to verify the identity and authenticity of the ID documents presented. If an introducer or suitable certifier has met the customer, they must confirm to the FSP that they have met the customer via video-conferencing, including a photograph or scanned copy of the documents. 16. Customer identification and transactions that rely on reliable independent digital ID systems with appropriate risk mitigation measures in place which have been approved by a credible body may present a standard level of risk. 17. FSPs shall adopt appropriate anti-fraud and cybersecurity measures to support digital ID/e-KYC technology, such as authentication systems for CDD purposes. **Inclusion of the definitions Digital ID system and E-KYC in the footnote:** • A digital ID system is a system that covers the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital.– FATF Guidance on Digital ID, 2020 • E-KYC refers to the processes whereby a customer's identity is verified via electronic means.
Section 3 D ***High-Risk Classification Factors***	<u>High-risk Classification Factors (Products, services and delivery channels)</u> 1. When assigning high risk ratings relating to products, services and delivery channels, FSPs should consider: (1) the level of transparency, or otherwise of the product, service or transaction (e.g. the extent to which the products or services facilitate or allow anonymity or opaqueness of the customer, ownership or beneficiary structures that could be used for illicit purposes); (2) non-face-to-face business relationships and/or occasional transactions when other high-risk factors have been identified. **Inclusion of the definition Video-conferencing in the footnote.** Video-conferencing is a live, visual, and audio method of communication between two or more remote parties over the internet that stimulates a face-to-face meeting.
Section 3 G (1)	**A. NEW PRODUCTS AND TECHNOLOGIES**

Reference:	**Proposed Amendment/New Provision**
Inclusion of 1(4) and section (2)	1. FSPs should have systems in place to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as: (1) digital information storage including cloud computing; (2) digital or electronic documentation storage; (3) electronic verification of documentation; (4) digital ID system/technology solutions; (5) data and transaction screening systems; or (6) the use of virtual or digital currencies. 2. FSPs should have robust documented policies and procedures in place to ensure a consistent and adequate approach to relying on existing or new digital ID system/technology solutions for CDD purposes. These may include (but are not limited to): a. A tiered CDD approach that leverages technology solutions with various assurance levels; b. Policies for the secure electronic collection and retention of records; c. A process for enabling authorities to obtain the underlying identity information and evidence needed for identification and verification of individuals; d. Anti-fraud and cybersecurity processes to support e-KYC/digital ID proofing and/or authentication for AML/CFT efforts; e. Back-up plans for possible instances where the technology solution fails; f. A description of risk indicators that would prompt a FSP to refrain from utilising digital ID system/technology solutions; and g. Procedures for the regular, ongoing, and independent review of the effectiveness of systems and processes used.
Section 4 Customer Due Diligence ***(New provisions 16 (d), 17 & 18)***	16. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, FSPs should: (1) Identify the applicant and verify its identity. The type of information that would normally be needed to perform this function would be: (a) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a

Reference:	**Proposed Amendment/New Provision**
	certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer. (b) The constitutional documents that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons holding a senior management position in the legal person or arrangement (e.g. directors, senior managing directors in a company, trustee(s) of a trust). (c) The address of the registered office, and, if different, a principal place of business. **(d) When verifying customers that are legal persons, regulated entities may use publicly available sources, including company registries.** 17. The use of video-conferencing to onboard customers who are legal persons or arrangements may be used to identify natural persons such as ultimate beneficial owners, settlors, trustees, protectors, or those appointed to act on behalf of the customer. 18. FSPs who are unable to verify official documents such as certificates of incorporation and trust deeds presented during video-conferencing or via other electronic methods due to unavailability of public sources must seek alternative measures to verify the documentation. This may include obtaining an original certified true copy or accepting soft copies digitally signed by a suitable certifier attesting to the authenticity of the documents.
Section 4 B ***Identification Information and Verification Procedures***	10. FSPs should have policies and procedures in place to address any specific risks associated with non-face to face [7]business relationships and transactions. **Inclusion of the definition of Non-face-to-face business relationships in the footnote**. Non-face-to-face business relationships – the establishment of business relationships and carrying out transactions where the customer is not physically present at the place where the relationship is being established or transaction is conducted. <u>Non-Face-to-Face</u> 35. Any interaction between an FSP and an applicant/customer in a non-direct manner increases the exposure to risk. Not only does this allow for

[7] Non-face to face business relationships – the establishment of business relationships and carrying out of transactions where the customer is not physically present at the place where the relationship is being established or transaction is conducted.

Reference:	**Proposed Amendment/New Provision**
Section 4 C	third parties to have access to assets or property through impersonation but may also disguise the true owner of that property by, for example, provision of false identification documentation. FSPs should put into place policies and procedures that appropriately address the risks posed by non-face-to-face contact for customers at the opening of the business relationship and through the operation of that relationship. 37. Where there are doubts around the veracity of identity verified electronically, or copy documents are used, an FSP should apply additional verification checks. For example, where it is impractical or impossible to obtain sight of original documents, a copy should only be accepted where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the applicant. **A. TIMING OF VERIFICATION[8]** 1. The best time to undertake verification is prior to entry into the business relationship or conducting a transaction. However, it could be necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed. FSPs may complete verification after the establishment of the business relationship, provided that: (1) This occurs as soon as reasonably practicable; (2) This is essential not to interrupt the normal conduct of business; and (3) The ML/TF risks are effectively managed. 2. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of long-term insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include: (1) Non-face-to-face business, **in accordance with a risk-based approach**.
Inclusion of New provision 20 and 21.	
Amendment of existing 20 (the new 21)	20. Certification of documents through "selfie" documents, photographs or videos**:** Photographs should clearly show the person's face and the image on the identity document being held in the same picture to demonstrate this actually belongs to the customer. A clear scanned copy or photograph of the document itself should also be provided. 21. CDD documents in electronic form, including government issued identification received in e-format are acceptable provided that the FSP takes a RBA and has suitable documented policies and procedures in place

[8] FATF- R.10 and IN 11 and 12

Reference:	**Proposed Amendment/New Provision**
	to ensure the authenticity of the electronic document(s). For further guidance, FSPs may refer to the Statement of Guidance on the '*Nature, accessibility and retention of records*' issued by the Monetary Authority, where applicable
Section 5 A ***Simplified Due Diligence Measures*** ***New provision 6***	6. FSPs may consider digital ID systems/e-KYC processes with lower levels of assurance to be sufficient for simplified due diligence in cases of low ML/TF risk.
Section 8 A ***New provision (3)***	3. FSPs must also ensure that records of identification data obtained through digital ID systems and e-KYC procedures are easily accessible, maintained and can be made available to competent authorities upon request.
Part V Section 1 H (7) (1) Insurance	7. It is recommended that EDD be applied for high risk situations and in situations where the insurer is particularly exposed to reputational risk. There will be certain occasions where EDD will be required, for example: (1) when there is an identified high-risk factor accompanied by no face-to-face contact with the insurer; (2) where the customer is a PEP; (3) where the beneficiary of a policy can be transferred; and (4) when the customer is involved in a business that is considered to present a high risk for ML/TF.
	Transactions <u>General</u> 1. The following are some of the warning signs and red flags that MRPs should be alert to in respect transactions generally. The list is not exhaustive, but includes: (1) The transaction seems to involve unnecessary complexity; (2) Use of front/straw men and/or shell companies; (3) Transactions in a series are structured just below the threshold for due diligence identity checks; (4) The customer appears to be trying to avoid reporting requirements by using two or more locations or

Reference:	**Proposed Amendment/New Provision**
Part VII Section 1 H 3 (21) ***MSB***	cashiers on the same day or in quick succession to break one transaction into smaller transactions; (5) Two or more customers appear to be trying to avoid reporting requirements and seem to be working together to break one transaction into two or more transactions; (6) Transactions are carried out by the customer on behalf of third parties without there being an appropriate business relationship with such parties; (7) Frequent transaction orders are made by the same customer; (8) Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation; (9) An unusually large (cash) transaction; (10) The amount of the transaction is unusually large for the typical customer or for the MSB; (11) The transaction has no apparent purpose or no obvious economic/financial basis; (12) Unnecessary routing of funds through third parties; (13) A customer sends/receives funds to/from him/herself, for no apparent purpose; (14) There is no genuine reason for the customer to use the services of the MSB; (15) Transfers of large sums of money to or from overseas locations with instructions for payment in cash; (16) One legal/natural person transfers sums to many legal/natural persons; (17) One legal/natural person receives sums from many legal/natural persons (from various countries); (18) Many legal/natural persons (who have no obvious blood/business relation) are beneficial owners of transfers ordered by one legal/natural person; (19) An under-aged person receives funds from many legal/natural persons and/or from different locations; (20) A customer sends/receives funds to/from counterparts located in jurisdictions which are known to be exposed to ML/TF risks, for example, drug trafficking, terrorism financing, smuggling; ~~(21) Non-face-to-face customers that are not physically present for identification purposes;~~

F. Jurisdictional Comparison

13. There have been considerable developments globally around remote onboarding in the financial services sector, and several regulatory bodies have issued non-face-to-face customer due diligence advisories to their regulated entities.

14. This section highlights the global developments surrounding remote onboarding in the financial services sector. The comparison is mainly focused on the treatment of non-face-to-face on boarding in other countries.

Table 1 – Summary of AML/CFT Regulations on Remote On-boarding

Country	Examples of types of identification	Examples of service/product providers	Examples of types of remote onboarding	Regulation
Singapore	Digital ID system	Singpass	Video conferencing/E-signatures supplemented with additional checks	The remote on-boarding and the use of electronic identification is permitted under AML/CFT. Non-face-to-face CDD measures issued in February 2022.
Hong Kong	Digital ID system	iAMSmart	Electronic channels such as mobile applications or internet supplemented with additional checks	The remote on-boarding and the use of electronic identification is permitted under AML/CFT. Remote on-boarding guidance issued in May 2021.
Cayman Islands[9]	Digital ID technologies (case by case basis) Via electronic means	Certification of documents through 'selfie' documents, photographs or videos E-format for bills/government identification	Video conferencing and other forms of electronic channels in accordance with RBA supplemented with additional checks	Proposed amendments to the Guidance Notes as seen in **Appendix 1** will permit the use of remote on-boarding.

G. Cost and Benefit Analysis

15. **Table 2** provides a summary of the estimated costs and benefits of the proposed guidance notes.

Table 2 – Estimated Costs and Benefits of Guidance Notes

	Costs	Benefits
CIMA	The Authority will incur the usual administrative costs associated with the following: - Conducting industry consultation; - amending the guidance notes; - gazetting and publishing of the revised guidance notes; and - training staff on updated amendments. These costs are not deemed to be overly burdensome and represent typical costs of the Authority carrying out its mandate.	Enhances, clarifies and supports the Authority's stance on FSPs' use of innovation and technology, thus preserving its competitive edge as a leading and forward-thinking offshore financial regulatory body.

[9] These are based on the proposed amendments to the guidance notes.

	Costs	Benefits
Cayman Islands	There are no immediate foreseen costs to the jurisdiction as a whole with the amendments made to the guidance notes. When legislation is approved and a formal Digital ID implemented, it may result in costs to the jurisdiction.	The amendments will promote ease of on-boarding clients in the Cayman Islands while supporting the growth of Cayman's digital society.
Regulated Entities	Staff training on using e-KYC methods and digital ID technologies as part of the risk-based approach. Administrative costs of implementing technologies for on-boarding clients.	The amendments will enable regulated entities to widen its reach to the unserved and underserved persons while reducing CDD related costs. Further, the proposed amendments will align regulated entities in the Cayman Islands with international best practices and standards relating to the use of e-KYC methods and digital ID technologies.

H. Consultation Feedback and Comments

16. Before proceeding with the proposed Measures, the Authority shall have regard to any representations made by the private sector associations only. Feedback submitted by individuals, entities, or other bodies, unless acting on behalf of private sector associations, will not be accepted by the Authority. Representations from private sector associations must be submitted as a consolidated document, and a listing of the entities which provided feedback should be included. Private sector associations should ensure that conflicting positions are resolved prior to submission to the Authority. Where positions conflict within or across associations, the Authority will consider all available information in taking a decision, which will be at its sole discretion.

17. To ensure that all responses are given due consideration, it is important that private sector associations make clear reference to the sections of the measure being commented on, and that responses are unambiguous, clearly articulated and based on fact. The consultation process is not designed to address complaints or grievances. Feedback of this nature should be submitted through the established complaints process.

18. In cases where the feedback proposes to change a policy position of the Authority or substantially amend any requirement of the draft measure, information to support the position of the association must be provided. The table below provides an example of the Authority's expectation with regard to feedback for the proposed measure.

Reference	Example of a Helpful Comment	Examples of Comments needing more Support
Rule 4.2[10]	In Rule 4.2 the current text omits the fair value measurement of liabilities. Also, as defined it is not asymmetrical with the Market Price definition and	× This is not what is done in other jurisdictions. × I don't think we should do this.

[10] This example is not reflective of the content of the proposed measure.

Reference	Example of a Helpful Comment	Examples of Comments needing more Support
	thus scenarios exists that fall into neither category. **<u>Suggested wording:</u>** *Hard-to-Value Securities means an asset <u>or liability</u> for which <u>there is no Market Price which is required to be measured at fair value pursuant to 5.2</u>*	× CIMA is not considering the position of the experts.

19. All feedback submitted by private sector associations will be given due consideration, nevertheless, the decision to adopt any feedback provided into a proposed measure will be at the sole discretion of the Authority.

I. Notice of Representations

20. The Authority seeks consultation through written comments and representations from the private sector associations concerning the proposed:

a) Amendments to Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (5 June 2020)– e-KYC and Remote CDD/Ongoing Monitoring ("Guidance Notes") (**Appendix 1)**.

21. The Authority must receive representations by 1700hrs on **February 1 2023**. Representations received after this deadline may not be considered and will not form part of the collated written response provided to private sector associations.

22. Comments and representations must be addressed to[11]:

The Managing Director
Cayman Islands Monetary Authority
P.O. Box 10052
SIX, Cricket Square
Grand Cayman KY1-1001
Cayman Islands
Tel: 345-949-7089
Fax: 345-946-5611
Email:
consultation@cima.ky
and copied to [charissaevelyn@cima.ky]

23. The Authority shall have due regard to any representation made by the private sector associations and industry stakeholders. The Authority shall provide a written response collating the feedback received and the Authority's position on this feedback. This response shall be copied to all relevant private sector associations only.

[11] Where the private sector association or industry stakeholder has no comments or representations on the proposed measure, it is recommended that the Authority be informed of this fact.

SIX, Cricket Square
PO Box 10052
Grand Cayman KY1 - 1001
CAYMAN ISLANDS

General Office: 345-949-7089

www.cima.ky