

## Capital Index (Global) Limited – Financial Crime Policy

Capital Index (Global) Limited (“CIG”) is a financial services company incorporated in the Bahamas, CIG is committed to maintaining effective prevention and detection measures to assist the law enforcement authorities in combating financial crime. This document sets out the policies which CIG has adopted to meet its legal obligations under relevant anti-money laundering and counter terrorist financing legislation.

CIG will seek to ensure that:

- clients and partners’ identities are satisfactorily verified in accordance with the firm’s risk-based approach before business is undertaken with them;
- it knows its clients and understands their reasons for doing business with us, both at the initial acceptance stage and throughout the business relationship;
- its employees are trained and made aware of both their personal legal obligations and the legal obligations of the firm;
- its employees are trained to be vigilant for activities where there may be reasonable grounds for suspicion that money laundering, terrorist financing or other adverse activity could be taking place and their responsibilities to disclose any suspicions to CIG’s Money Laundering Reporting Officer (“MLRO”);
- sufficient records are retained for the required retention periods; and
- adequate procedures are established, maintained and implemented to achieve these objectives.

Money laundering, terrorist financing and fraud threats are dynamic, and criminals constantly devise new techniques and exploit the easiest targets in the financial services sector. To mitigate the risk of being used as a vehicle for financial crime CIG will systematically assess, mitigate and monitor these risks. CIG will seek to identify fraud, money laundering and terrorist financing at an early stage of the client acceptance process and escalate this to the MLRO and take appropriate action.

The risk-based approach adopted by CIG will be the driver of our overall strategy of fighting financial crime. Through this approach, we will identify the areas of greatest vulnerability and focus our resources on those areas. Ultimate responsibility for this approach lies with the senior management but all employees carry a responsibility to maintain the effectiveness of systems and controls employed by the firm.

### Financial Crime Risk

CIG’s regulator – the Securities Commission of Bahamas (“SCB”) financial crime objective encompasses the prevention of financial fraud, market abuse and money laundering. Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds.

Money laundering and terrorist financing risks are closely related to the risks of fraud and insider dealing. While these are separate offences, money laundering involves handling the proceeds of any crime, including the proceeds of these activities.

The ability to launder the proceeds of crime through the financial system is vital to the success of criminal operations. But firms that become involved in money laundering risk prosecution or regulatory enforcement sanctions which potentially damage their reputation or brand.

To reduce the incidence of financial crime the procedures that CIG has adopted focus on knowing our clients, understanding their businesses, carrying out proportionate verification checks and identifying and reporting suspicious activity.

### Law, Regulation and Industry Practice

CIG is subject to the laws of The Bahamas and rules set by the SCB. The SCB provides practical interpretation of legal and regulatory requirements and indicates good industry practice. CIG has taken these laws and guidelines into account when devising a risk-based approach to the prevention of money laundering.

The laws of The Bahamas specifically concerning money laundering and terrorist financing is contained in the following legislation:

- the Proceeds of Crime Act, 2000 (“POCA”) (as amended);
- the Anti-Terrorism Act, 2004 (as amended);
- the Financial Transactions Reporting Act, 2000 (as amended) (“FTRA”);
- the Financial Transactions Reporting Regulations, 2000 (as amended) (“FTRR”);
- the Financial Transactions Reporting (Wire Transfers) Regulations, 2009;
- the Financial Intelligence Unit Act, 2000 (as amended) (“FIUA”);
- the Financial Intelligence (Transactions Reporting) Regulations, 2001 (as amended);
- the Securities Industry Act, 2011 (as amended) (“SIA”); and,
- the Securities Industry (Anti Money Laundering and Countering the Financing of Terrorism) Rules, 2015 (as amended) (“SIR”)

### General Principles

In order to comply with the laws, regulations and guidance, CIG has adopted the following principles:

#### *Money Laundering Reporting Officer*

CIG has appointed a Money Laundering Reporting Officer (“MLRO”). The MLRO acts as the central point of contact with the external agencies such as the Financial Intelligence Unit (“FIU”) and law enforcement agencies, and internally, in relation to all matters relating to financial crime. The MLRO monitors CIG’s compliance with the firm’s anti-money laundering procedures and submits reports to the Board at least on an annual basis. The MLRO is an approved person under the regulator’s Approved Persons regime.

#### *Risk-based Approach*

CIG has implemented policies, procedures and controls aimed at deterring criminals from using CIG for financial crime. These policies and procedures are tailored to the risk posed by individual clients, in accordance with the SIR.

### *Verification of Client Identity*

CIG has established Client Due Diligence (“CDD”) procedures to identify the users of its services and the principal beneficial owners and origins of funds used in these relationships. These procedures include knowing the nature of our clients’ and partners’ businesses and being alert to abnormal activity.

### *Suspicious Transactions*

Unexplained or abnormal transactions or activities that are suspected of being linked to criminal activity are reported to the MLRO without delay using. The MLRO then determines whether to report the suspicions to relevant external agencies.

### *Record-Keeping*

CIG is required by legislation to retain all records of transactions and the verification of identity of our clients for at least five years following the end of the business relationship. CIG keeps records of training provided to staff and the timing and form of training sessions. We also retain the records of any internal reports of suspicion submitted to the MLRO and any disclosures made to external agencies.

### *Training*

All employees are informed of their individual and collective responsibilities and CIG’s money laundering policies. Personnel are provided with training to enable them to understand the vulnerabilities of CIG’s business and to recognise and report suspicious activities.