Anti- Money Laundering and Counter-Terrorism Financing
Disclosure Statement

1. Institucional Information

• **Legal name:** Banco Interatlântico, S.A.

• **Principal place of business/legal address:**

Chã de Areia

CP 131 – A - Praia

Santiago, Cabo Verde

• **SWIFT BIC Code:** CGDI CV CP

• **Legal status:** Joint-stock company

• **Shareholders:**

Shareholders	% of Share
CAIXA GERAL DE DEPÓSITOS, S.A.*	81,69%
Others	18,31%

* Caixa Geral de Depósitos, S.A. (100% State owned company, plc – State of Portuguese Republic)

• **Regulators:** Banco de Cabo Verde (www.bcv.cv) e Auditoria Geral do Mercado de Valores Mobiliários (https://www.bcv.cv/pt/Supervisao/Mercado%20de%20Capitais/Paginas/Mercado-de-Capitais.aspx)

• **Financial Institution Register:** 5

• **External Auditors:** Ernest & Young Audit & Associados - SROC, S.A

• **AML Contact** – Gabinete de Função de *Compliance*

Address: Chã de Areia, CP 131-A - Santiago, Cabo Verde

Phone: 238 260 25 43

E-mail address: gfc@bi.cv

2. Relevant International and National Framework

International Framework:

- 40 Recommendations of FAFT/GAFI (developed in 1990, revised in 1996, 2003, 2004 and 2012) – that provide a complete set of counter-measures against money laundering and terrorist financing covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation.

Nacional Framework:

- Law nº 85/III/90 of October 6 - public control of political office holders indicating the positions applicable to these holders, as well as the obligations to which they are subject;
- Law nº 78 / IV / 93 of June 12 - Drug Law;
- Law nº. 119 / VIII / 2016 of 24 March - amends Law 27 / VIII / 2013 of 21 January establishing preventive and repressive measures against terrorism and it´s financing;
- Law no. 120 / VIII / 2016 of 24 March - amends Law 38 / VIII / 2009 of 27 April establishing measures to prevent and suppress the crime of money laundering, property, rights and obligations;
- Decree-Law nº 9/2012 of 20 March - regulates the organization, competence and operation of the Financial Information Unit – FIU;
- Official Notice Nº 5/2017 of September 7 (issued by capverdean banking supervisory, Bank of Cabo Verde) – where the procedures to be put in place by banks are defined, regarding customer identification, record keeping and the reporting of suspicious transaction;
- Criminal Code;
- Securities Code.

3. Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Measures in BI

BI has adopted internal policies, procedures and controls to ensure that it complies with AML/CTF obligations in existing legislation and regulations.

BI has adopted an AML/CFT program that reasonably identifies, mitigates and manages the risk of money laundering and terrorism financing. This program has been approved by BI´s Board of Directors.

Being Cabo Verde a member country oh the GIABA (and this member of GAFI) and because BI is a subsidiary of CGD, it also applies the following policies and procedures:

Customer Due Diligence/Know Your Customer: BI has policies and procedures in place to comply with the obligation to identify and perform due diligence on customers which includes a filtering IT solution (to check and watch proscribed lists) and is implementing an IT solution to score customer's profile based on ML/TF risk.

Politically Exposed Persons (PEPs): BI has enhanced due diligence and transaction screen towards customers or beneficial owners who are PEPs.

Holders of other political or public positions: BI has enhanced due diligence and transaction screen towards customers or beneficial owners who are holders of other political or public positions as defined in Official Notice 5/2017 (Bank of Cabo Verde).

Anonymous and numbered accounts: BI does not provide customers with anonymous or numbered accounts.

Record Keeping: Records relating to customer identification and original documents, copies, references or any other durable support systems, equally admissible in court proceedings as evidence, of the demonstrative documents and of the records of the transactions, are kept to enable the reconstruction of the transaction, for a period of seven (7) years after its execution, even if the transaction is part of a business relationship that has already ended.

Monitoring of Suspicious Activities: Screening of customer's transactions is carried out by an IT solution through a risk-based approach and also by the BI's workers.

Reports of Suspicious Transactions: BI is required to report any suspicious customer activities or transactions to PGR – Procurador Geral da República (Republic's General Attorney) and to UIF – Unidade de Informação Financeira (Financial Intelligence Unit). Internal policies and procedures are in place to ensure compliance with the applicable legislation and regulatory requirements.

Reports of significant account and non-account based cash transactions and all IMTs: BI is required to report significant account cash transactions over CVE 1.000.000 (or less, if suspicious) to those entities and to the regulatory authority IMT to offshore jurisdictions. Details of all IMTs (wire transfers) such as sender and beneficiary names and address are checked against watch lists. Internal policies and procedures are in place to ensure compliance with the applicable legislation and regulatory requirements.

Employee Training Program: AML/CFT training is provided to all units. Staff involved in customer facing areas receive special training and reminders on the detection and reporting process for suspicious activities.

Employee due diligence: BI has processes that provide reasonable assurance of the identity, honesty and integrity of prospective and existing employees.

Independent audit and compliance review function: Our internal auditors and the compliance department conduct programs of audit and compliance tests of all BI's policies and operational procedures including those applicable to AML. The audit and compliance programs are approved by the Board of Directors.

Correspondent Banks: BI has implemented risk based due diligence procedures that include the following – understanding the nature of the correspondent's business, its license to operate, the quality of its management, ownership and effective control, its AML policies, external oversight and prudential supervision including it's AML/CFT regime. Additionally, ongoing due diligence of correspondent accounts is performed on a regular basis or when circumstances change. All correspondent banking relationships are approved by the Board of Directors and subject to binding advice of CGD.

Shell Banks: BI does not conduct business with shell banks, as defined in the AML/CFT law. Nº 120/VIII/2016.

Payable-through accounts: BI doesn't provide payable through accounts because our policies and procedures prohibit offering this kind of services as defined in the AML/CFT.

Assessment of payments against watch lists and proscribed lists (TF and sanctions): BI has an IT solution to filter all inward and outward payments against UN, EU and OFAC proscribed lists.

Sanctions Policy: BI has implemented a set of policies and procedures to ensure that the institution does not establish or maintain a business relationship, or process operations to / for the benefit of persons, entities or sanctioned countries.

Please find 'Sanctions Policy' in the website (www.bi.cv).

5. Wolfsberg AML Questionnaire

BI follows the principles contained in Wolfsberg AML Questionnaire concerning AML/CTF.

The Wolfsberg AML Questionnaire BI is available in the website (www.bi.cv).

6. USA Patriot Act Certificate

Under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act 2001, BI may be required from time to time to provide Certification Regarding Accounts for Foreign banks.

Please find 'USA Patriot Act Certificate' in the website (www.bi.cv).

Banco Interatlântico, S.A.

September 19, 2022